



Model Number: M505N

Product Description: ADSL2+ / Ethernet WAN Residential Gateway featuring:

Qty 4 10/100 Ethernet Port

Qty 1 USB 2.0

802.11b/g/n 2T2R

To Contact VisionNet for Tier 2 Support:

Voice: + 1 925 730 3940

Email: support@visionnetusa.com

Online: <http://www.visionnetusa.com/ticketportal>

TABLE OF CONTENTS

SECTION 1: GUI ACCESS

1.1	Accessing the GUI	4
-----	-------------------	---

SECTION 2: TROUBLESHOOTING

2.1	View WAN Statistics	6
2.2	View WAN Details	7
2.3	View DSL Statistics	8
2.4	View ATM Statistics	9
2.5	View DHCP Statistics	10
2.6	View ARP Statistics	11
2.7	View LAN Statistics	12
2.8	Verify Connectivity via Ping	13
2.9	Verify Connectivity via Trace Route	15
2.10	Remote / Local System Log Recording	17
2.11	PPP Debug System Logging	19
2.12	NAT Inspection via Command Line Interface	20

SECTION 3: WAN CONFIGURATION

3.1	Changing DSL Parameters	21
3.2	WAN Logic Overview	22
3.3	Selecting a WAN Interface to Create	23
3.4	Creating a DSL Interface	24
3.5	Creating a PTM Interface	25
3.6	Creating an Ethernet Interface	26
3.7	Creating an IPoE WAN Service	28
3.8	Creating a PPPoE WAN Service	30
3.9	Creating a Bridge WAN Service	36
3.10	WAN Interface Prioritization	38
3.11	Gateway Prioritization	39
3.12	Universal Static Gateway Service	40
3.13	DNS Prioritization	41
3.14	Universal Static DNS Service	43

SECTION 4: PUBLIC WAN IP ADDRESS ALLOCATION

4.1	Public IP Allocation - Public Subnet (WAN Interface within Subnet)	45
4.2	Public IP Allocation - Virtual Public Subnet (WAN Interface not within Subnet)	48
4.3	Public IP Allocation - 1:1 NAT Public Subnet	52
4.4	Public IP Allocation - PPPIP Extension (Single Public IP)	56

SECTION 5: LAN CONFIGURATION

5.1	LAN Service Configuration	58
5.2	Reserving a Public IP Address	59
5.3	IGMP Force	60

SECTION 6: SECURITY CONFIGURATION

6.1	Port Forwarding	61
6.2	Port Triggering	64
6.3	DMZ Host	68
6.4	UPnP	69
6.5	Algorithm Enable / Disable	70
6.6	WAN Access Control (Parental Control)	71
6.7	URL Filtering (Parental Control)	72
6.8	IP Filtering	73
6.9	Bridge Access Control	74

SECTION 7: QUALITY OF SERVICE

7.1	QoS Enable / Disable	75
7.2	QoS Interface Configuration	76
7.3	QoS Classification	77

SECTION 8: SERVICE GROUPING

8.1	Service Group Logic	78
8.2	Service Group Creation	79
8.3	Service Group LAN Management	80

SECTION 9: CONFIGURATION SETTINGS

9.0	Configuration File Logic	81
9.1	Save Backup Configuration	82
9.2	Over-Writing the Default Configuration	83
9.3	Update the Running Configuration	84
9.4	Restoring the Default Settings	85
9.5	Updating the Modem Firmware	87
9.6	Rebooting the Modem	88
9.7	ACS Configuration	89
9.8	SNMP Configuration	90
9.9	NTP Configuration	91
9.10	IP Restriction (Management ACLs)	92
9.11	Remote Access	93

SECTION 10: WI FI

10.1	Wireless Channel Configuration	94
10.2	SSID Configuration	95
10.3	Wireless Configuration	96
10.4	Global Settings	97
10.5	MAC Filtering	99
10.6	Wireless Bridge	100

SECTION 11: PRODUCT DEPICTIONS AND BEHAVIOR

11.1	LED Behavior	101
11.2	Product Depiction	102

SECTION 12: Troubleshooting

12.1	Port Mirroring	103
------	----------------	-----

SECTION 1: GUI ACCESS

Section 1.1 – Accessing the GUI

Step 1: Accessing the GUI via a web browser

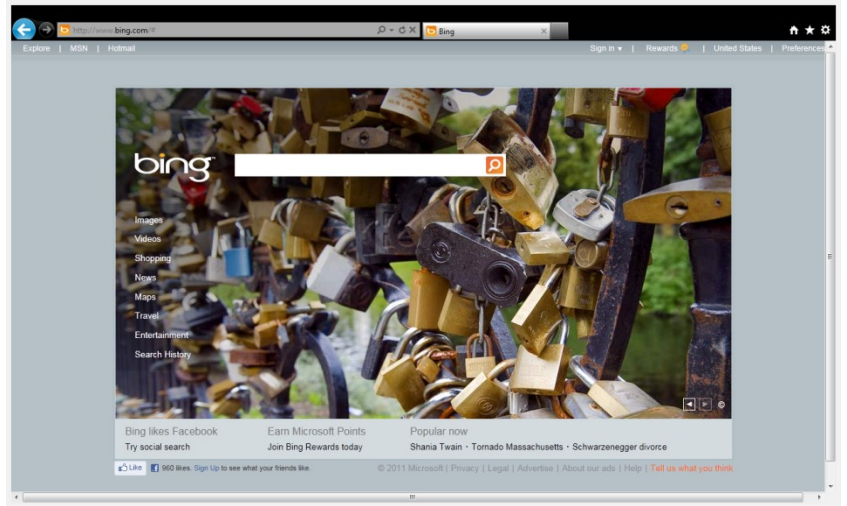
1.A Open your Web Browser

Enter the WAN IP Address of the device in the address bar to access the modem remotely

ie: <http://67.125.108.137>

Use the modem's LAN IP Address to access the GUI locally

<http://192.168.1.254>



1.B Once the modem responds, you will be challenged for a User Name and Password

Remote Access

Privileged

Username: support
Password: ISP Specific

Restricted

Username: techsupport
Password: ISP Specific

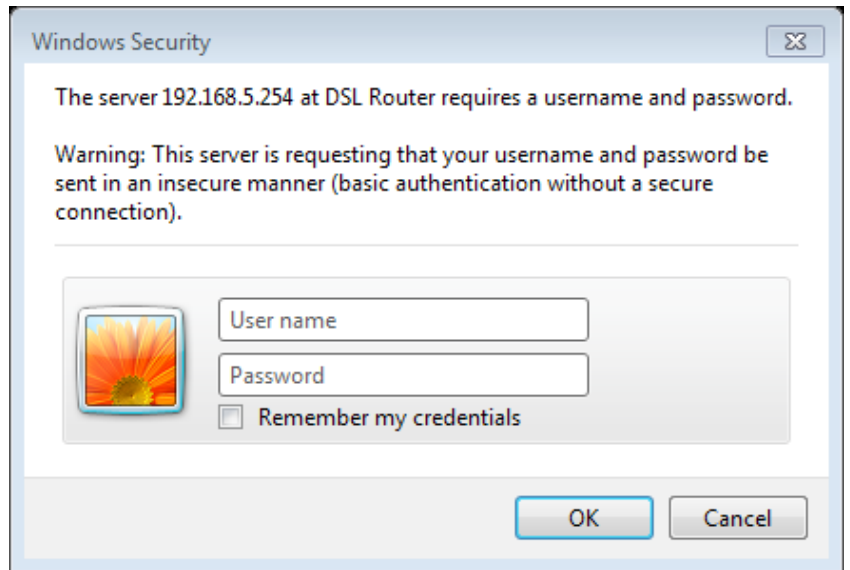
Local Access

Privileged

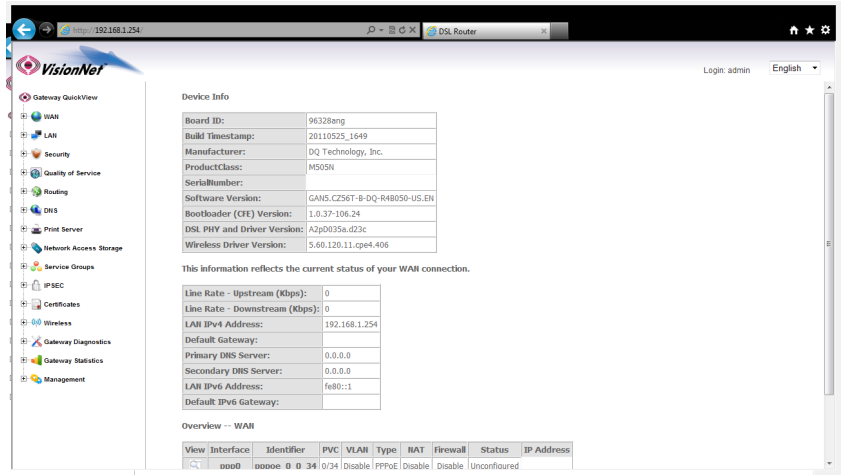
Username: admin
Password: ISP Specific

Restricted

Username: enduser
Password: password



1. C You will be directed to the Main GUI Page



 **PLEASE NOTE:**

ONLY the End User Login should be given to End Users. NEVER RELEASE ANY OTHER LOGIN INFORMATION.

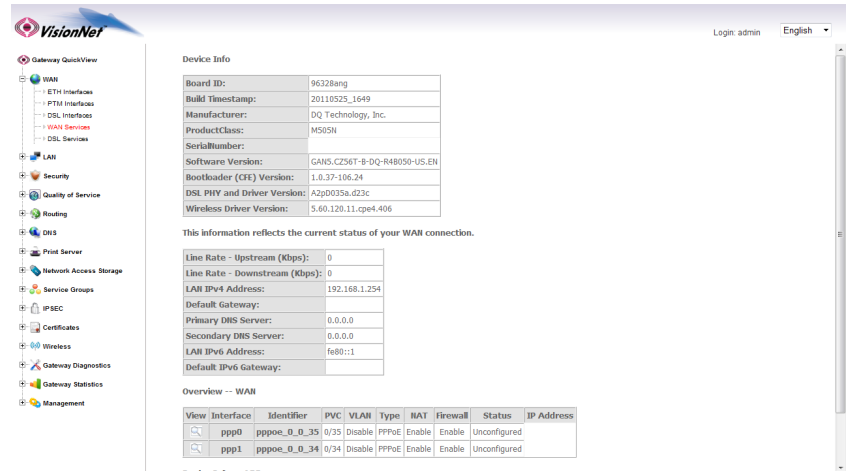
SECTION 2: TROUBLESHOOTING

Section 2.1 – View WAN Status

Step 1: Access the GUI to find the WAN Status

- 1.A Select the **“Gateway Quickview”** tab located within the left-hand frameset.

Then, scroll to the **“Overview – WAN”** Section



The screenshot shows the VisionNet Gateway QuickView interface. On the left is a navigation tree with 'WAN' selected. The main content area displays 'Device Info' with fields for Board ID, Build Timestamp, Manufacturer, Product Class, Serial Number, Software Version, Bootloader (CFE) Version, DSL PHY and Driver Version, and Wireless Driver Version. Below this is a section for WAN connection status, including Line Rate (Upstream/Downstream), LAN IPv4 Address, Default Gateway, and DNS Servers. At the bottom, an 'Overview -- WAN' table lists interfaces ppp0 and ppp1 with their respective PVC, VLAN, Type, RAT, Firewall, Status, and IP Address.

View	Interface	Identifier	PVC	VLAN	Type	RAT	Firewall	Status	IP Address
	ppp0	pppoe_0_0_35	0/35	Disable	PPPOE	Enable	Enable	Unconfigured	
	ppp1	pppoe_0_0_34	0/34	Disable	PPPOE	Enable	Enable	Unconfigured	

- 1.B

At least one WAN Service should be “Up”.

Status:

If there is not an “up” link, then there will be no WAN Access

Only one WAN Service should have an IP Address

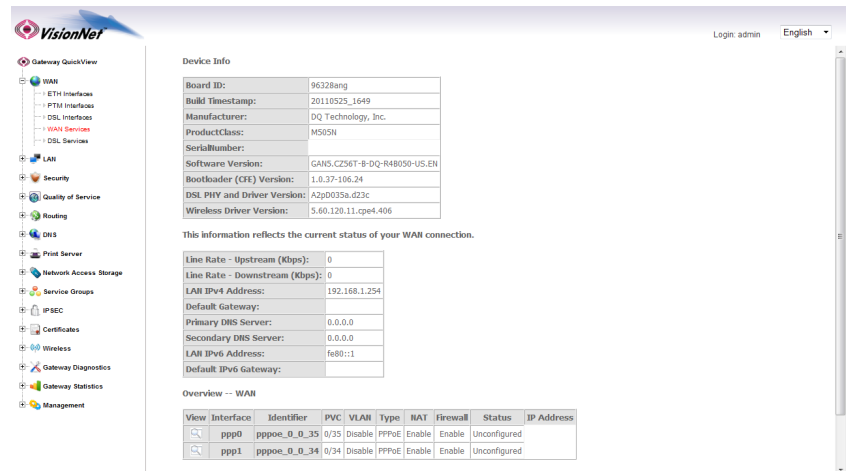
IP Address:

Without a WAN IP address, there will be no WAN Access.

(With exception of Bridged Connections)

Protocol:

ISP Specific



This screenshot is identical to the one in 1.A, showing the VisionNet Gateway QuickView interface with the WAN status overview table.

View	Interface	Identifier	PVC	VLAN	Type	RAT	Firewall	Status	IP Address
	ppp0	pppoe_0_0_35	0/35	Disable	PPPOE	Enable	Enable	Unconfigured	
	ppp1	pppoe_0_0_34	0/34	Disable	PPPOE	Enable	Enable	Unconfigured	

WHAT THESE STATISTICS MEAN:

This page will verify that the WAN connection is operating correctly, and that the modem has obtained a WAN IP Address

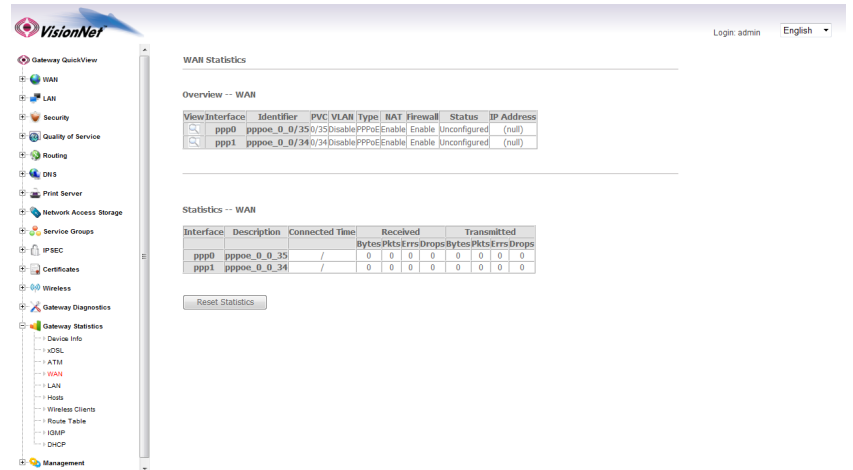
Section 2.2 – View WAN Statistics

Step 1: Access the GUI to find WAN Statistics

- 1.A Select the **“Gateway Statistics”** tab located within the left-hand frameset.

Then, scroll to the **“WAN”** Section

Select the  icon next to the active WAN connection



WAN Statistics

Overview -- WAN

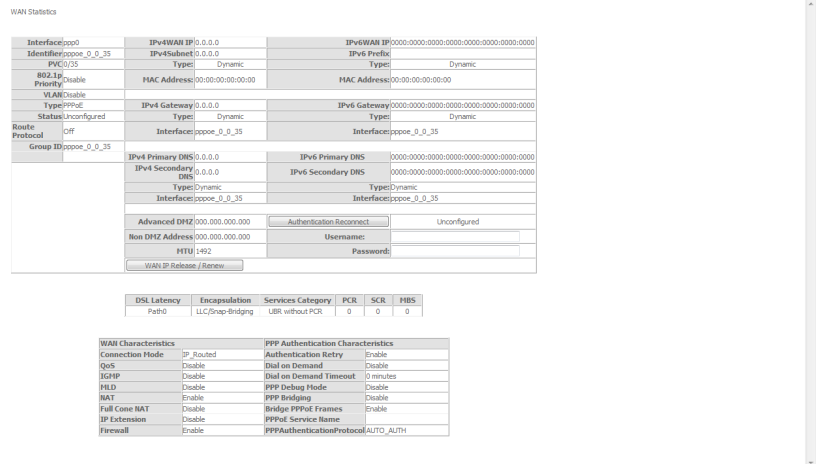
View Interface	Identifier	PVC	VLAN	Type	NAT	Firewall	Status	IP Address
ppp0	pppoe_0_0_35/0/35	Disable	PPPoE	Enable	Enable	Unconfigured	(null)	
ppp1	pppoe_0_0_34/0/34	Disable	PPPoE	Enable	Enable	Unconfigured	(null)	

Statistics -- WAN

Interface	Description	Connected	Time	Received			Transmitted					
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops	
ppp0	pppoe_0_0_35	/		0	0	0	0	0	0	0	0	0
ppp1	pppoe_0_0_34	/		0	0	0	0	0	0	0	0	0

Reset Statistics

- 1.A Select the **“Gateway Quickview”** tab located within the left-hand frameset.



WAN Statistics

Interface	IPv4 WAN IP	IPv6 WAN IP
ppp0	0.0.0.0	0000:0000:0000:0000:0000:0000:0000:0000
pppoe_0_0_35	0.0.0.0	0000:0000:0000:0000:0000:0000:0000:0000
PPPoE	Type: Dynamic	Type: Dynamic
Bonding	MAC Address: 00:00:00:00:00:00	MAC Address: 00:00:00:00:00:00
VLAN	Disable	Disable
Type	PPPoE	IPv6 Gateway
Status	Unconfigured	Type: Dynamic
Route	Off	Interface: pppoe_0_0_35
Protocol	Group ID: pppoe_0_0_35	Interface: pppoe_0_0_35
IPV4 Primary DNS	0.0.0.0	IPv6 Primary DNS
IPV4 Secondary DNS	0.0.0.0	IPv6 Secondary DNS
Type	Dynamic	Type: Dynamic
Interface	pppoe_0_0_35	Interface: pppoe_0_0_35
Advanced DHCP	0000:0000:0000:0000	Authentication Reconnect
Non DHCP Address	0000:0000:0000:0000	User Name
MTU	1492	Password
WAN IP Release / Renew		

DSL Latency	Encapsulation	Services Category	PCR	SCR	MBS
Path0	LLC/Snap-Bridging	UBR without PCR	0	0	0

WAN Characteristics	PPP Authentication Characteristics
Connection Mode	IP Routed
QoS	Disable
IGMP	Disable
MFD	Disable
NAT	Enable
Full Cone NAT	Disable
IP Extension	Disable
Firewall	Enable

WHAT THESE STATISTICS MEAN:

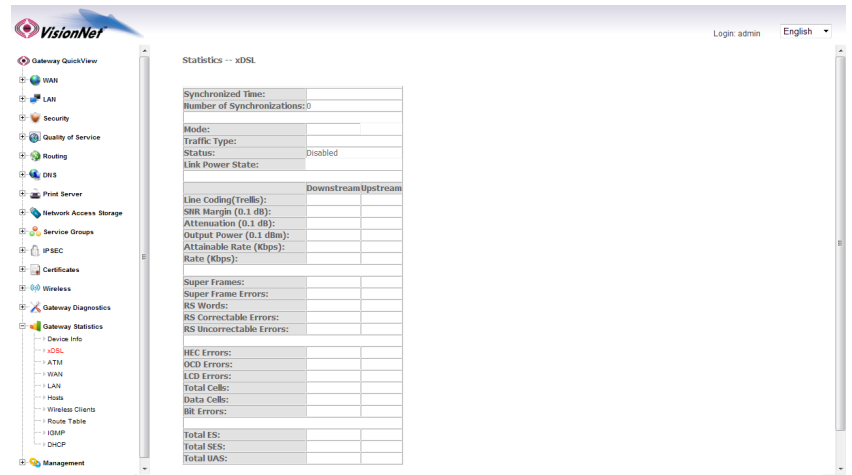
This page will verify that data is being received and transmitted. You will also be able to view detailed IPV4, IPV6, and Configuration Settings

Section 2.3 – View DSL Statistics

Step 1: Access the GUI to find DSL Statistics

- 1.A Select the **“Gateway Statistics”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“xDSL”**



The screenshot shows the VisionNet GUI. The left-hand frameset contains a navigation tree with the following items: Gateway QuickView, WAN, LAN, Security, Quality of Service, Routing, DNS, Print Server, Network Access Storage, Service Groups, IPSEC, Certificates, Wireless, Gateway Diagnostics, Device Info, xDSL, ATM, WAN, LAN, Hosts, Wireless Clients, Route Table, IGMP, DHCP, and Management. The 'Gateway Diagnostics' folder is expanded, and 'xDSL' is selected. The main content area displays the 'Statistics -- xDSL' page. The page title is 'Statistics -- xDSL'. The page contains a table of statistics for xDSL. The table has two columns: 'Downstream' and 'Upstream'. The statistics are as follows:

	Downstream	Upstream
Synchronized Time:		
Number of Synchronizations:	0	
Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:		
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:		
QCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
RR Errors:		
Total ES:		
Total SES:		
Total UAS:		

! WHAT THESE STATISTICS MEAN:

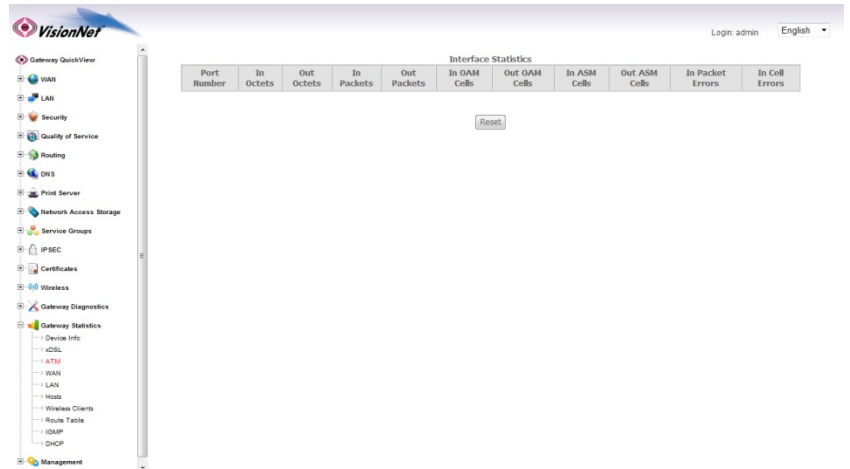
This page will verify DSL Link, and will provide information regarding line characteristics and capacities.

Section 2.4 – View ATM Statistics

Step 1: Access the GUI to find ATM Statistics

- 1.A Select the **“Gateway Statistics”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“ATM”**



The screenshot shows the VisionNet GUI. On the left is a navigation tree with the following items: Gateway QuickView, WAN, LAN, Security, Quality of Service, Routing, DNS, Print Server, Network Access Storage, Service Groups, IPSEC, Certificates, Wireless, Gateway Diagnostics, Gateway Statistics, Device Info, ADSL, ATM, ISDN, LAN, Hosts, Wireless Clients, Route Table, HMAP, and DHCP. A blue arrow points to the 'Gateway Statistics' item. The main content area is titled 'Interface Statistics' and contains a table with the following columns: 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, and In Cell Errors. A 'Reset' button is located below the table.

WHAT THESE STATISTICS MEAN:

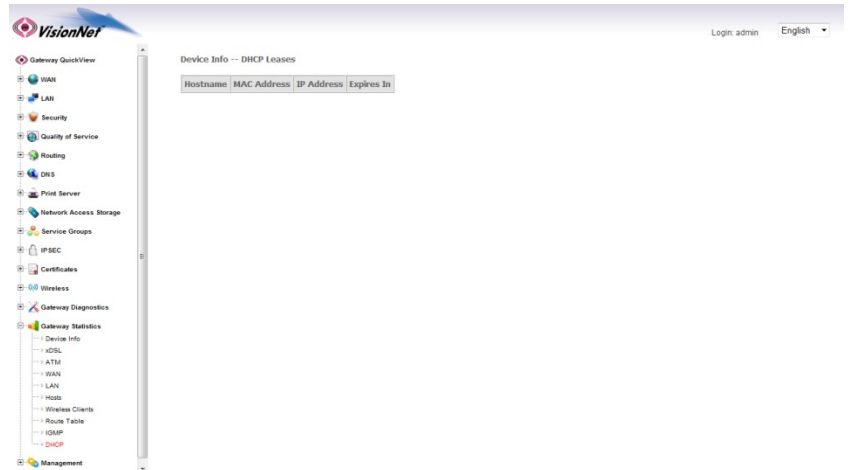
This page will verify ATM Operation, and specify the type of packets being sent

Section 2.5 – View DHCP Statistics

Step 1: Access the GUI to find DHCP Statistics

- 1.A Select the [“Gateway Statistics”](#) tab located within the left-hand frameset.

Then, In the left-hand frameset, select [“DHCP”](#)



WHAT THESE STATISTICS MEAN:

This page will provide the IP Addresses assigned by the modem's DHCP server, the MAC addresses of dynamically assigned devices, and the amount of time that the device has spent on the network.

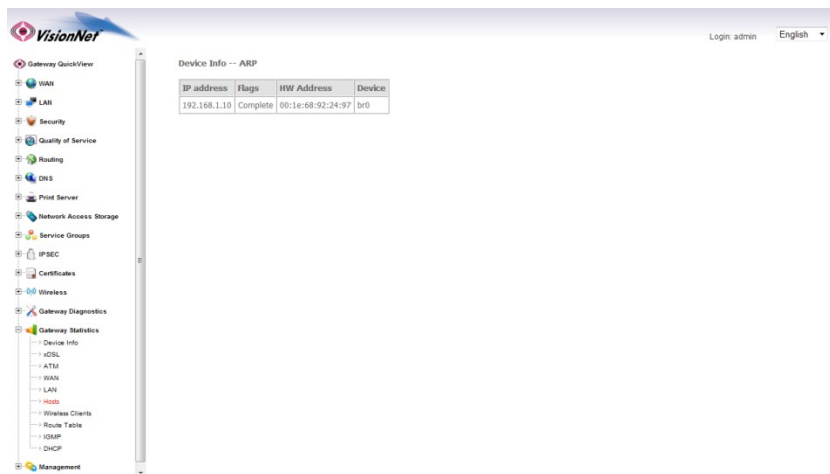
Section 2.6 – View ARP Statistics

Step 1: Access the GUI to find ARP Statistics

This step may be used to view all connected LAN devices, and is especially useful when using the “Reserve an IP Address” feature.

- 1.A Select the [“Gateway Statistics”](#) tab located within the left-hand frameset.

Then, in the left-hand frameset, select [“Hosts”](#)



WHAT THESE STATISTICS MEAN:

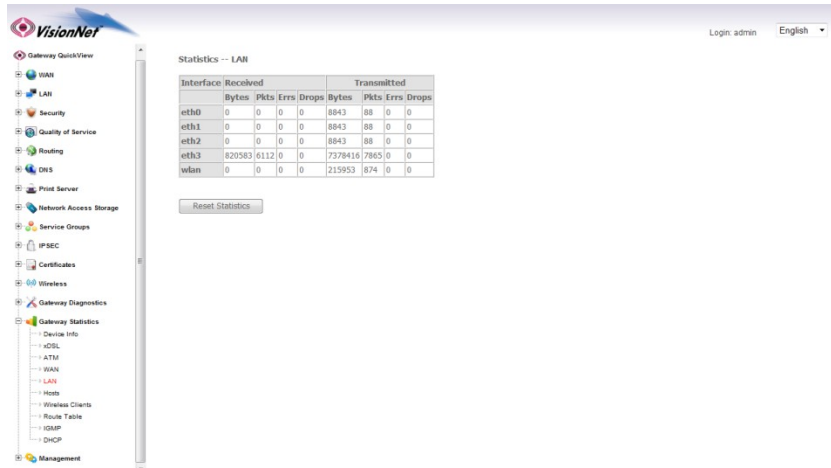
This page will provide the MAC Addresses of all recognized devices connected to the modem. A device will only be recognized once it has requested data from the modem.

Section 2.7 – View LAN Statistics

Step 1: Access the GUI to find LAN Statistics

- 1.A Select the **“Gateway Statistics”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“LAN”**



Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	8843	88	0	0
eth1	0	0	0	0	8843	88	0	0
eth2	0	0	0	0	8843	88	0	0
eth3	820583	6112	0	0	7378416	7865	0	0
wlan	0	0	0	0	215953	874	0	0

Reset Statistics

WHAT THESE STATISTICS MEAN:

This page will verify that LAN Devices are communicating.

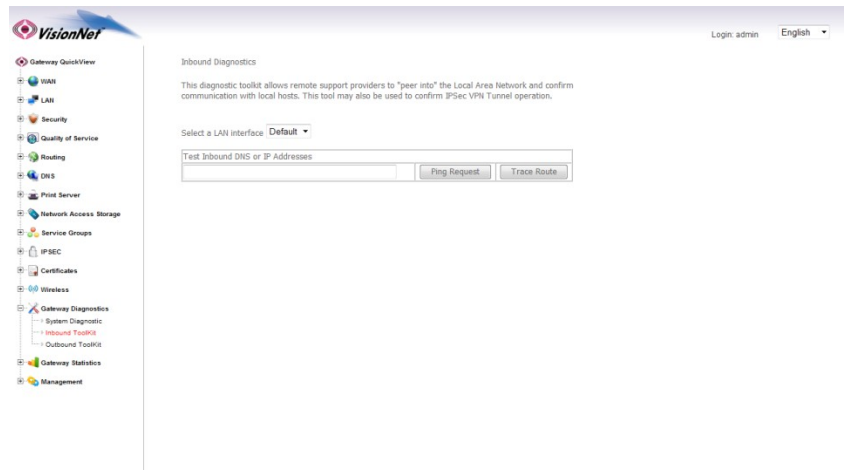
Section 2.8 – Verify Connectivity via Ping

In the event that you cannot access a LAN client, or access an internet page, you may wish to use the Ping command to test the connection.

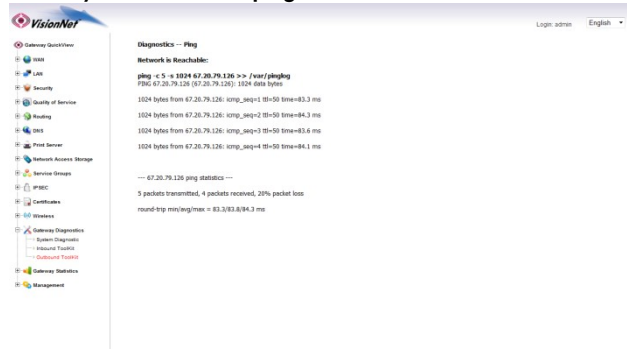
Step 1: Access the GUI to find the Ping Tool

- 1.A Select the **“Gateway Diagnostics”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select either **“Inbound Toolkit” (LAN)** or **“Outbound Toolkit” (WAN)**



- 1.B You may use this tool to ping either a domain name or an IP Address



TO TEST LOCAL LAN DEVICES:

Enter the IP Address of the LAN Device and select **“Ping Request”**

ie: 192.168.1.64

TO TEST REMOTE WAN IP ADDRESSES:

Enter the WAN IP Address and select **“Ping Request”**

ie: 4.2.2.4

TO TEST REMOTE WAN DOMAIN NAMES:

Enter the Domain Name and select **“Ping Request”**

ie: www.bing.com

If you can Ping a local device:

The local device has an IP Address (this does not guarantee that the Device has WAN Access)

If you can Ping the WAN Gateway:

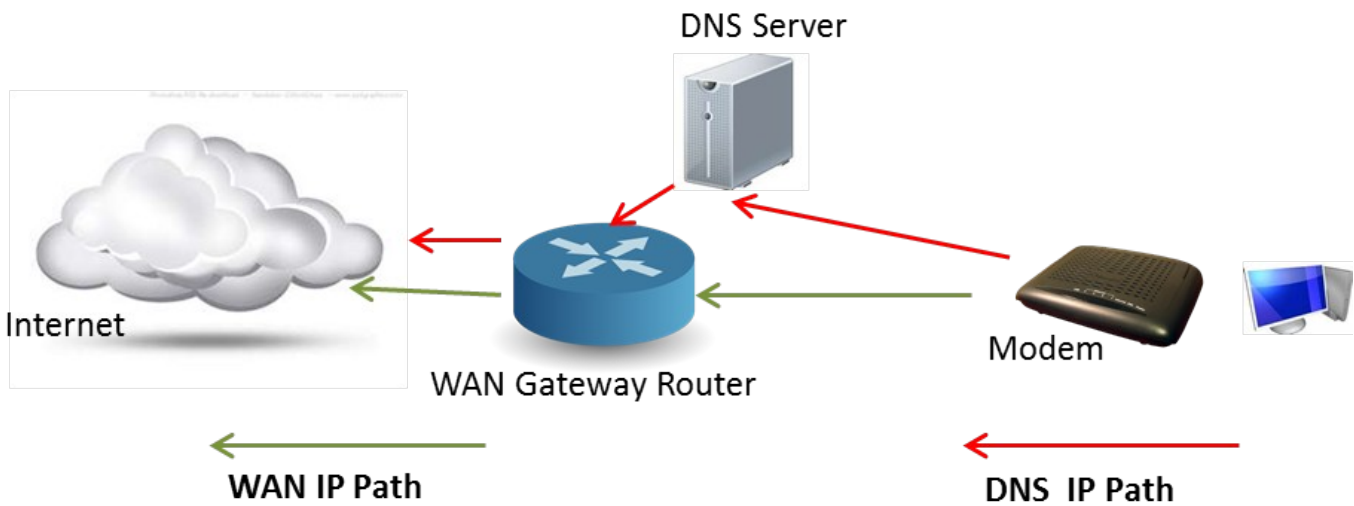
The modem's DHCP Client has properly obtained an IP Address

If you can Ping a WAN IP Address:

The modem can access the internet, but this does not necessarily mean that DNS resolution is operational

If you can Ping a WAN Domain Name

The modem can access the internet correctly



Section 2.9 – Verify Connectivity via Trace Route

In the event that you cannot access a web page, or have sporadic internet access even though the WAN gateway is operating correctly, you may perform a Trace Route.

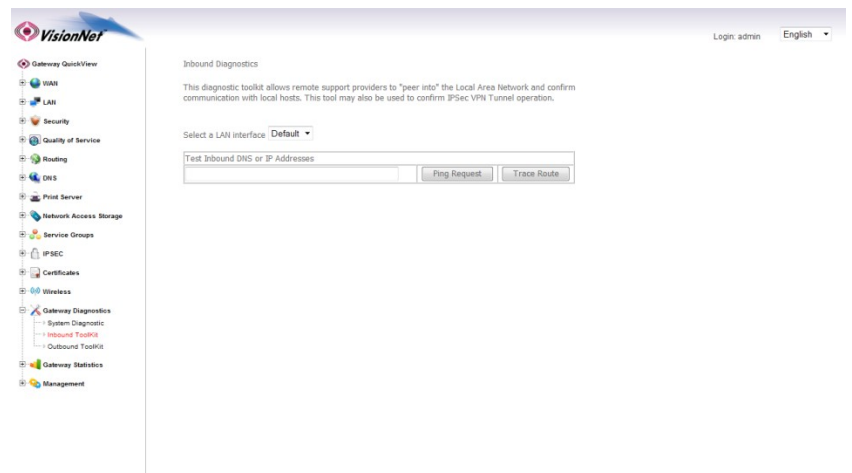
⚠ Please Note that the Trace Route function takes several minutes, and you cannot navigate away from the page during this process.

Step 1: Access the GUI to find the Trace Route Tool

- 1.A Select the **“Gateway Diagnostics”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select either **“Inbound Toolkit”**

(LAN) or **“Outbound Toolkit”**
(WAN)



- 1.B You may use this tool to trace the path of either a domain name or an IP Address

TO TEST LOCAL LAN DEVICES:

Enter the IP Address of the LAN Device and select **“Trace Route”**

ie: 192.168.1.64

This test should not show more than one “hop”

TO TEST REMOTE WAN IP ADDRESSES:

Enter the WAN IP Address and select **“Trace Route”**

ie: 4.2.2.4

This test will show you the path of the data being sent to the internet.

IP Addresses are not checked against a DNS Server

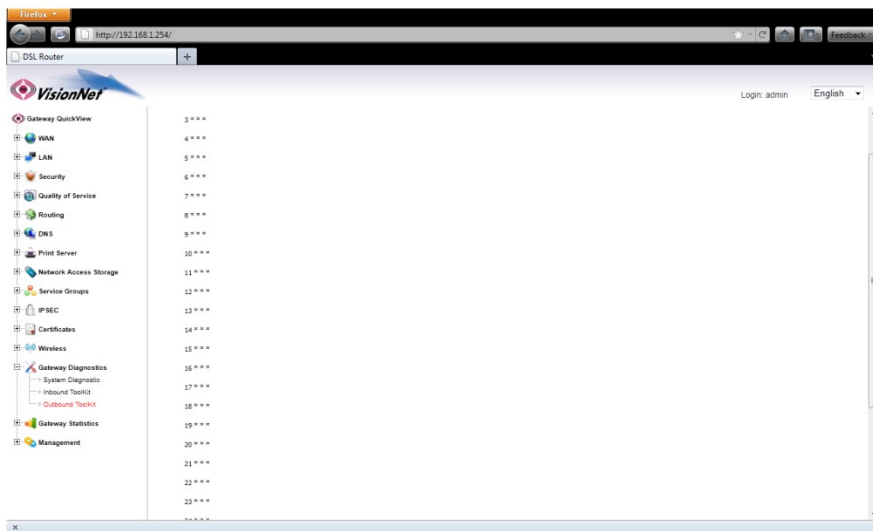
TO TEST REMOTE WAN DOMAIN NAMES:

Enter the Domain Name and select **“Trace Route”**

ie: www.google.com

This test will show you the path of the data being sent to the internet

This path includes resolving the Domain Name with a DNS Server

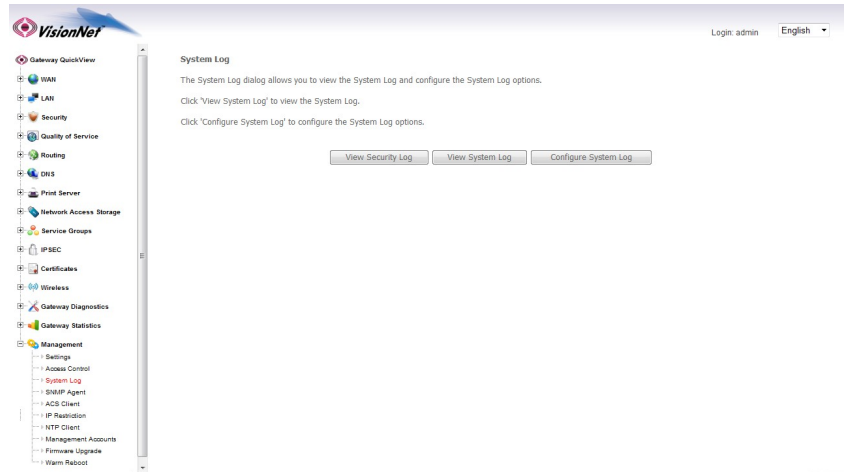


Section 2.10 – Local / Remote System Logging

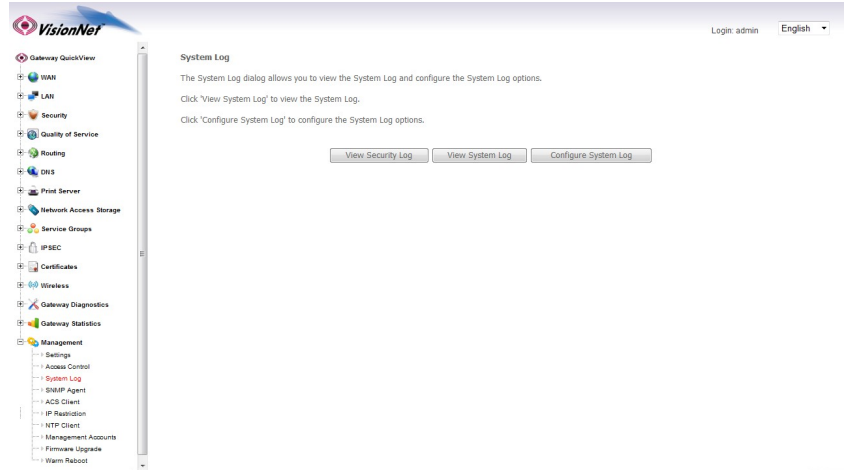
Step 1: Access the GUI to begin SysLog Configuration

- 1.A Select the **“Management”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“System Log”**



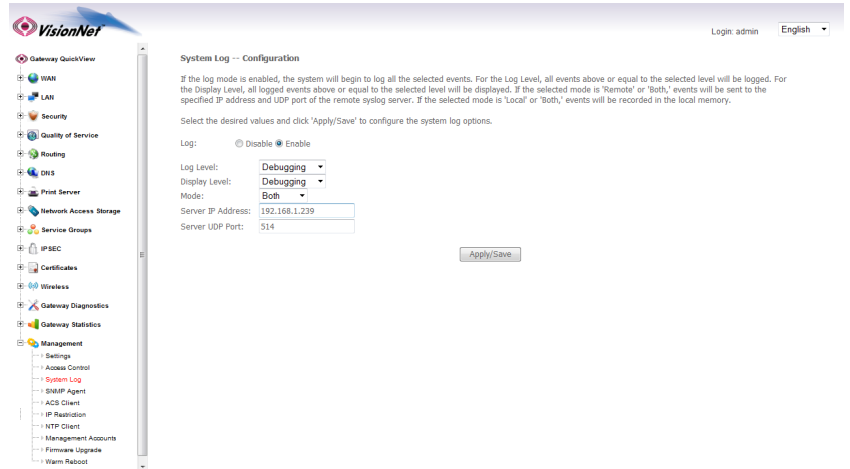
- 1.B Select the **“Configure System Log”** Button



Step 2: Configure the System Log

2.A Enable the System Log

Log:	Enabled
Mode:	Both Enables Internal and PC Server Logging
Log and Display Levels:	Debugging
Server IP Address:	Default 192.168.1.239 This must match the IP of the computer running Kiwi VisionNet suggests that the computer running Kiwi be statically assigned to 192.168.1.239
Server UDP Port:	514



2.B Select "Save/Apply"

Section 2.11 – PPP Debug for System Logging

Step 1: Select the appropriate WAN Service for modification

- 1.A Select the **“WAN”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“WAN Services”**

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	edit
ppp1	pppoe_0_0_34	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	edit

- 1.B Select the **“Edit”** Button associated with the relevant PVC (ie: 0/34 or 0/35)

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	edit
ppp1	pppoe_0_0_34	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	edit

- 2.A Edit the PPP Authentication Page

PPP DEBUG Enabled

PPP Username and Password

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: **AUTO**

MTU(10-1500):

Enable NAT

Enable Fullcone NAT

Enable Firewall

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

- 2.B Proceed through the remainder of the edit section.

PLEASE NOTE: THIS IS TEMPORARY ONLY, AND MUST NOT BE LEFT AS A PERMANENT CONFIGURATION

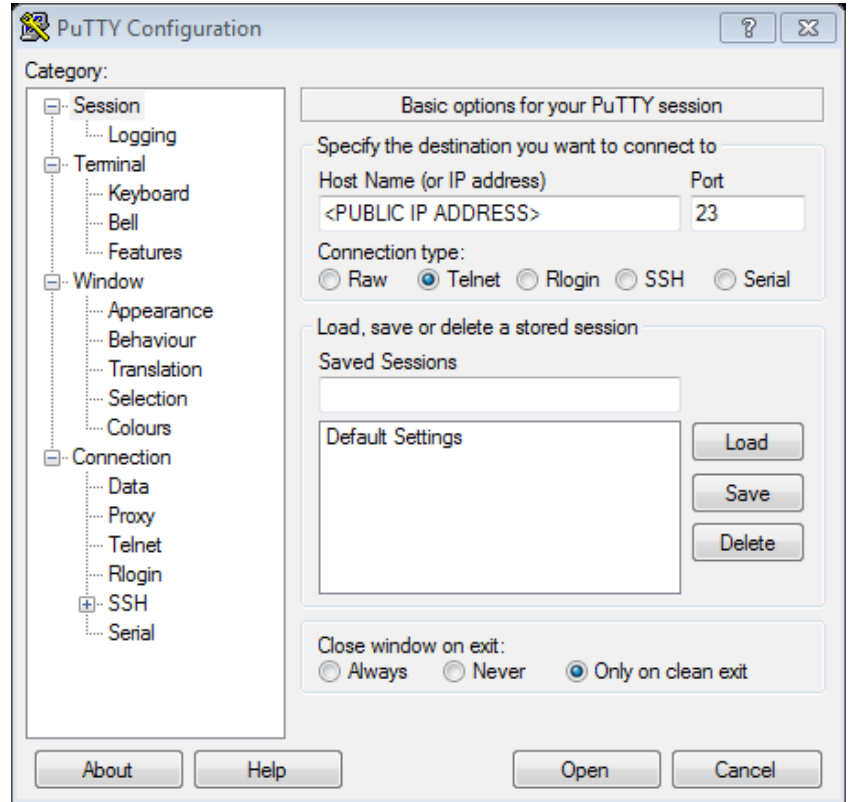
Section 2.12 – NAT INSPECTION VIA COMMAND LINE

Step 1: Open a Telnet Client

1.A Point the Telnet Client at the IP Address of the CPE

LOCAL: Use the private IP Address

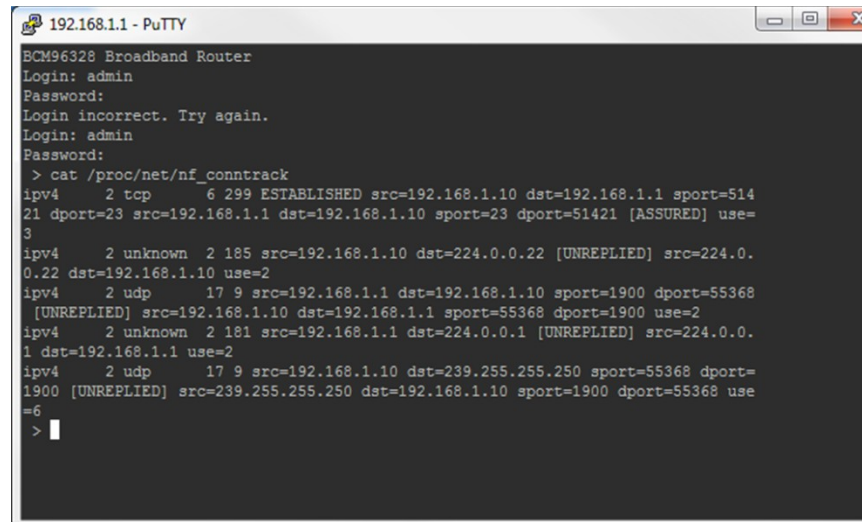
REMOTE: Use the public IP Address



1.B Login using the appropriate username and password

Enter the following command:

`cat /proc/net/nf_conntrack`



SECTION 3: WAN CONFIGURATION

Section 3.1 – Changing DSL Parameters

VisionNet modems come pre-configured with the following DSL Settings

DSL Protocol	Status
G.DMT	Enabled
G.Lite	Enabled
T1.413	Enabled
ADSL2	Enabled
ADSL2+	Enabled
Annex L	Enabled
Annex M	Disabled
Bitswap	Enabled
SRA	Disabled
PhyR	Disabled

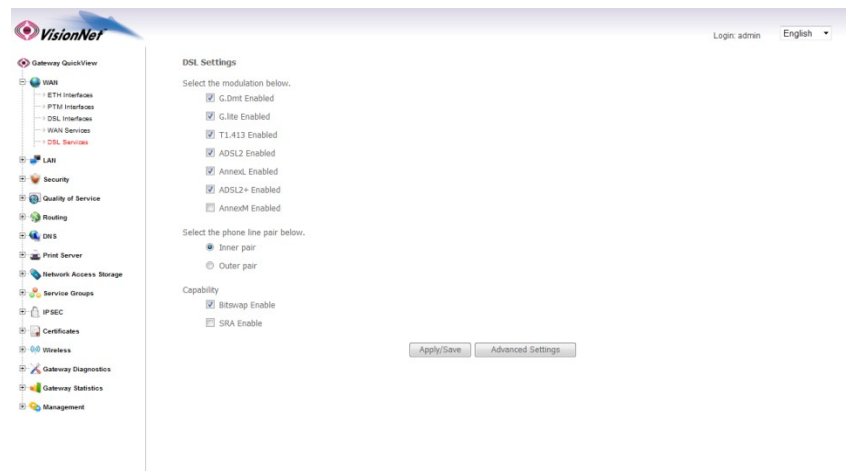
ALL VDSL2 PROTOCOLS ARE ENABLED, BY DEFAULT, FOR VDSL2 CPEs

During troubleshooting, you may be requested to change DSL Modulation settings. The below instructions will guide you through making these changes.

Step 1: Direct Your Browser to the LAN Configuration Page

- 1.A Select the **“WAN”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“DSL Services”**



- 1.B For Each DSL Protocol, a checked box indicates that it is enabled; while an unchecked box indicates that it is disabled.

- 1.C Only select **“Inner Pair”** under the section titled **“Select the Phone Line Pair”**.

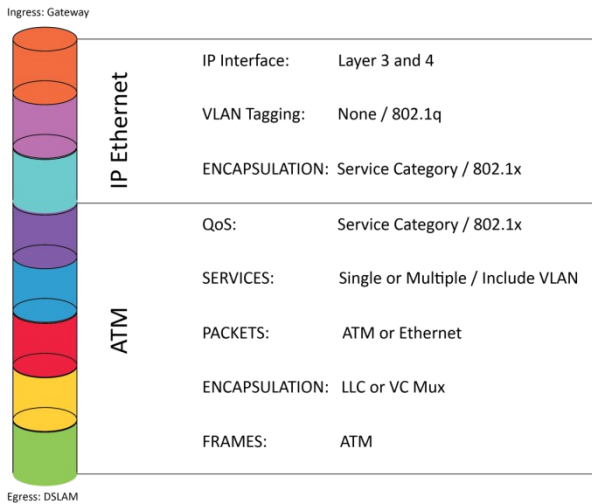
Changing these settings will change physical characteristics that may prevent proper operation and/or troubleshooting in the future.

Section 3.2 – WAN Logic and Theory

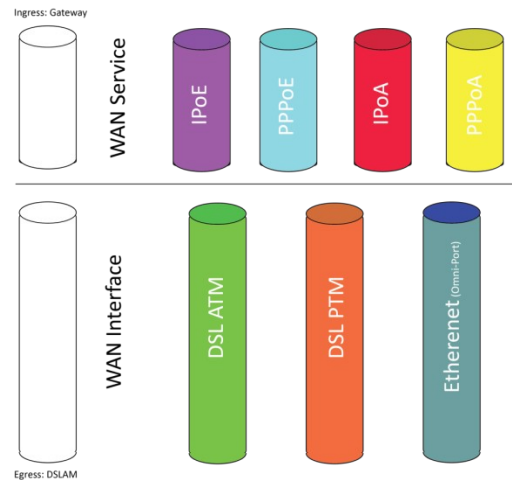
WAN INTERFACE / SERVICE CONSTRUCTION AND DECONSTRUCTION – A BRIEF INTRO

In the past, creating a WAN Service was a single operation in which the WAN Interface and WAN Service were created at the same time. This was because there was only one WAN Interface to choose from. Now that there are multiple WAN Interfaces to choose from, you must create the WAN Interface and the WAN Service separately.

PREVIOUS METHOD



NEW METHOD



SO WHAT CHANGED?

VisionNet Gateways now support

- ATM (Traditional DSL)
- PTM (Used for VDSL2 and PTM over ADSL2+)
- Ethernet (Used for Ethernet WAN Port Operation)

Which means that there are now two separate processes

BUILDING A WAN SERVICE

Create WAN Interface → Create WAN Service associated with WAN Interface

TEARING DOWN (REMOVING) A WAN SERVICE

Delete WAN Service associated with WAN Interface → Delete WAN Interface

Section 3.3 – Selecting a WAN Interface to Create

The VisionNet modem comes pre-configured. Unless you have VLAN Mux Enabled, you can only use one interface per physical port. Hence, do not attempt to build a new interface until you have removed any conflicting interfaces.

Step 1: Selecting the WAN Interface to Create

- 1.A Select the **“WAN”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select the appropriate WAN Interface

[“DSL”](#)

[“Ethernet”](#)

[“PTM”](#)



Section 3.4 – Creating a DSL Interface

Step 1: Selecting the WAN Interface to Create

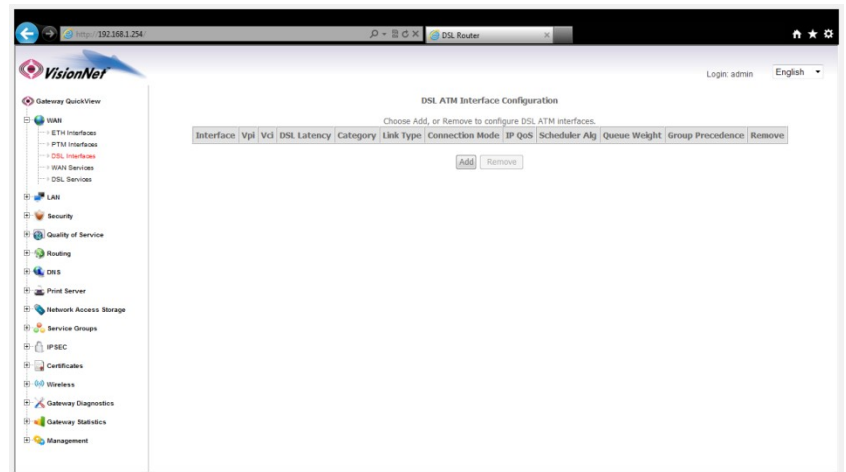
- 1.A Select the [“WAN”](#) tab located within the left-hand frameset.

Then, in the left-hand frameset, select the appropriate WAN Interface

[“DSL Interfaces”](#)



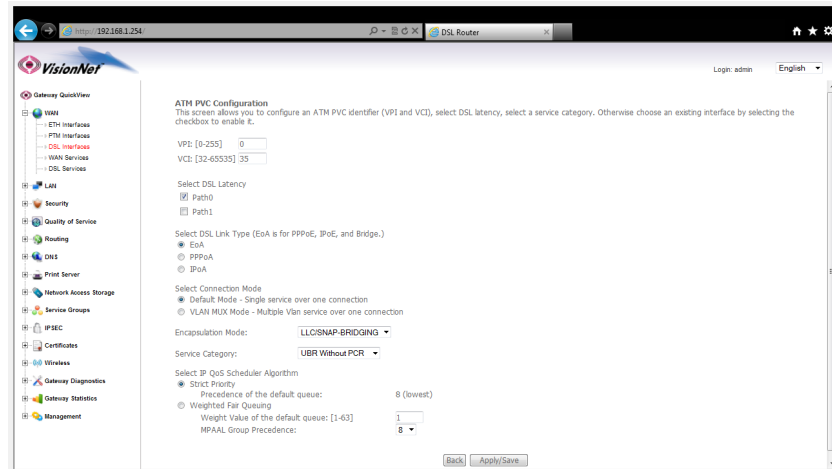
- 1.B Select [“Add”](#)



Step 2: Configuring the WAN Interface

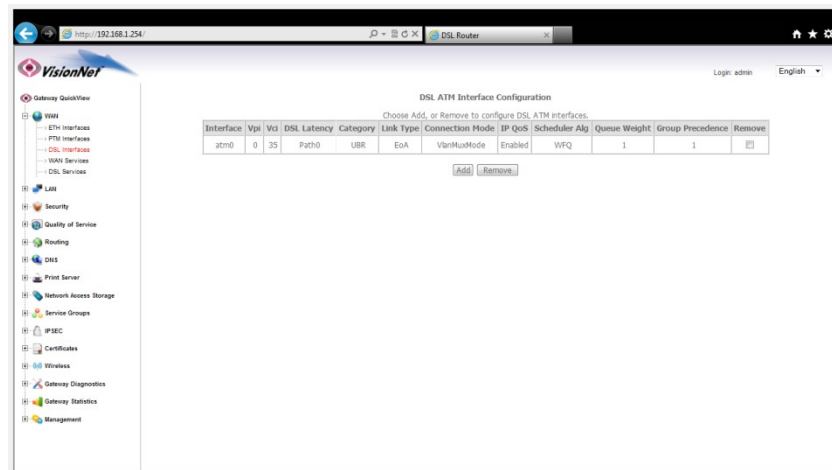
2.A Select the **“WAN”** tab located within the left-hand frameset.

VPI:	ISP Specific
VCI:	ISP Specific
DSL Latency	ONLY Path0 Should be checked EoA
Select DSL Link	IPOE/MER, PPPOE, Bridged PPPoA IPoA
Select Connection Mode:	Default Mode Standard (Single Service) VLAN MUX Multiple VLANs over a single PVC
Encapsulation Mode:	ISP Specific
Service Category:	ISP Specific Strict Policy Standard for single service config
Select ISP QoS	Weighted Fair Queuing Use multiple service configurations IE: Data PVC – 1/8 IE: IPTV PVC – 1/1



2.B Select **“Apply Save”**

You will see the Interface reflected in the updated Interface Table



Section 3.5 – Creating a PTM Interface

Step 1: Selecting the WAN Interface to Create

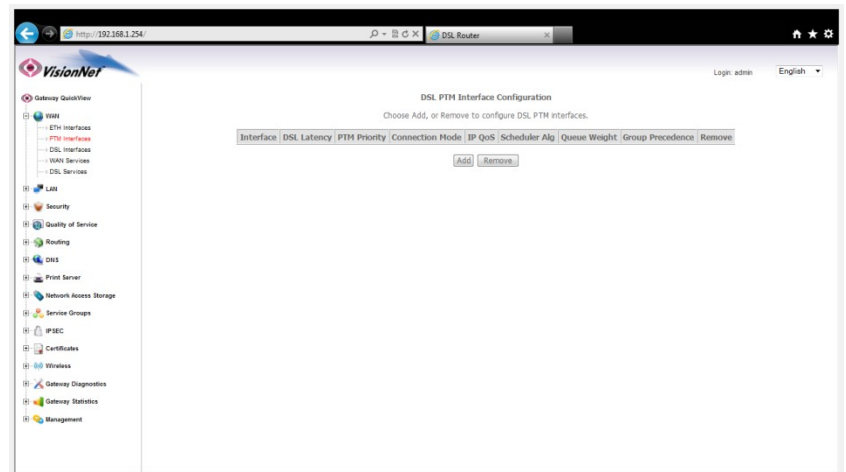
- 1.A Select the “WAN” tab located within the left-hand frameset.

Then, in the left-hand frameset, select the appropriate WAN Interface

“PTM Interfaces”



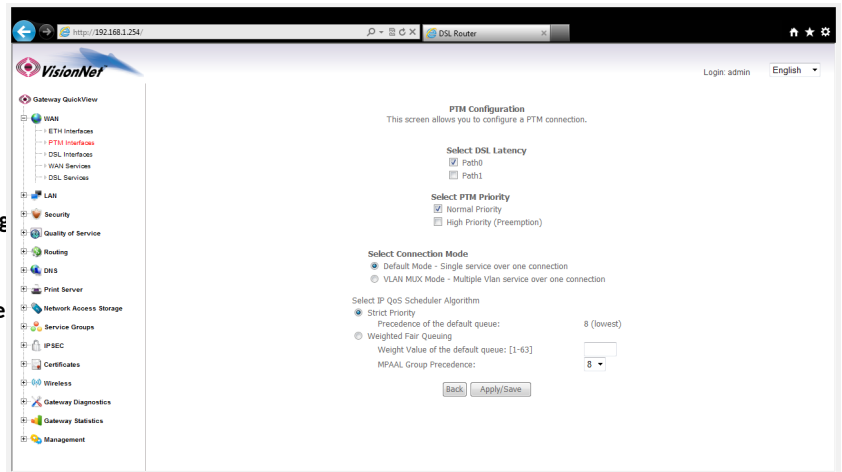
- 1.B Select “Add”



Step 2: Configuring the WAN Interface

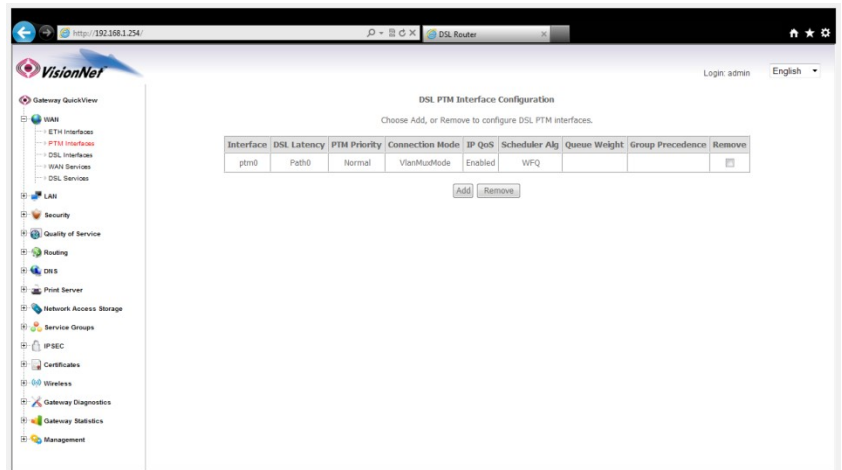
2.A Select the **“WAN”** tab located within the left-hand frameset.

DSL Latency	ONLY Path0 Should be checked
Select PTM Priority	<p>Normal Priority</p> <p>High Priority (Pre-Emption)</p> <p>Default Mode Standard (Single Service)</p>
Select Connection Mode:	<p>VLAN MUX</p> <p>Multiple VLANs over a single PVC</p> <p>Strict Policy</p> <p>Standard for single service config</p>
Select ISP QoS	<p>Weighted Fair Queuing</p> <p>Use multiple service configurations</p>



2.B Select **“Apply Save”**

You will see the Interface reflected in the updated Interface Table



Section 3.6 – Creating an Ethernet Interface

Step 1: Selecting the WAN Interface to Create

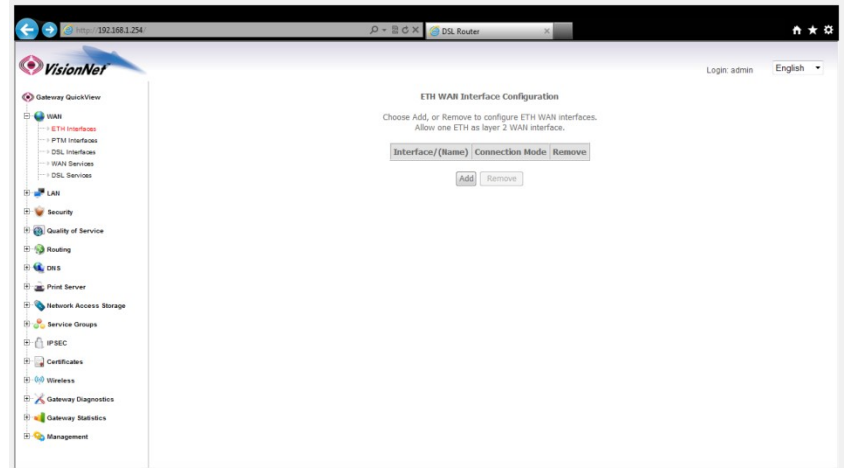
- 1.A Select the “WAN” tab located within the left-hand frameset.

Then, in the left-hand frameset, select the appropriate WAN Interface

“Ethernet Interfaces”



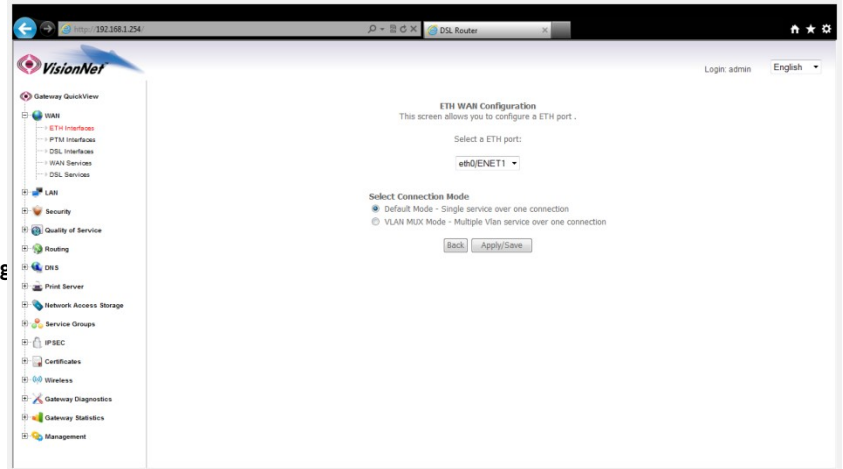
- 1.B Select “Add”



Step 2: Configuring the WAN Interface

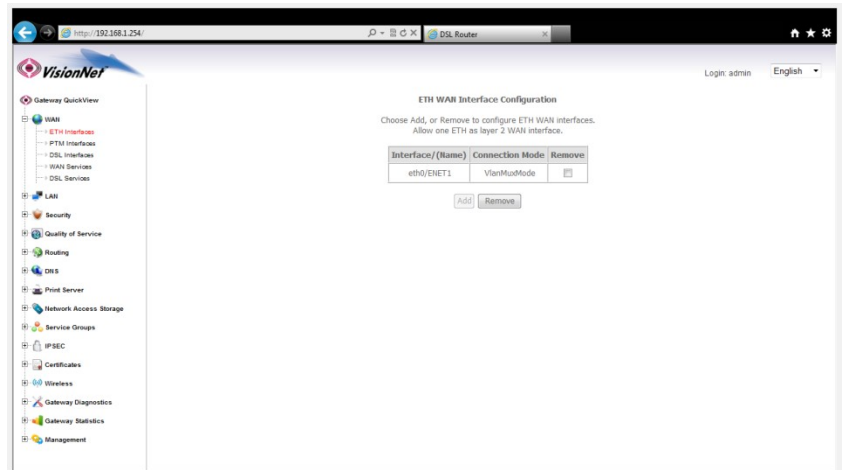
2.A Select the **“WAN”** tab located within the left-hand frameset.

Select Connection Mode:	ENET 1 - 4 ENET 4 Default OmniPort Default Mode Standard (Single Service)
Select Connection Mode:	VLAN MUX Multiple VLANs over a single PVC



2.B Select **“Apply Save”**

You will see the Interface reflected in the updated Interface Table



Section 3.7 – Creating an IPOE WAN Service

Step 1: Selecting the WAN Service to Create

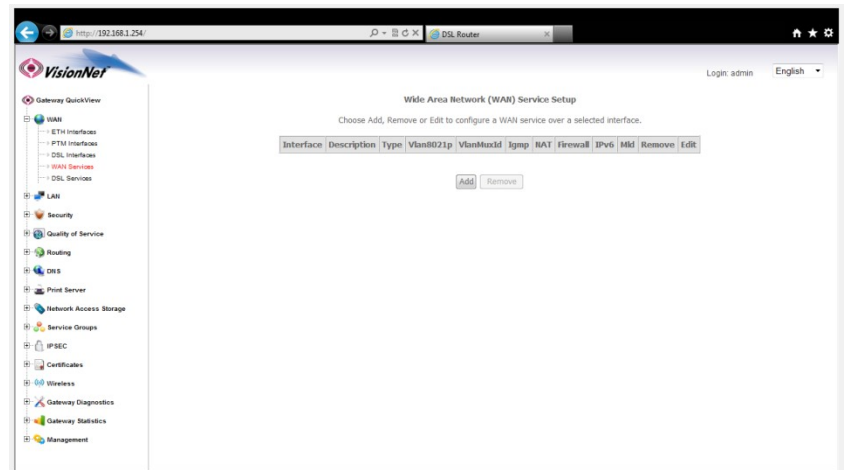
- 1.A Select the **“WAN”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select the appropriate WAN Interface

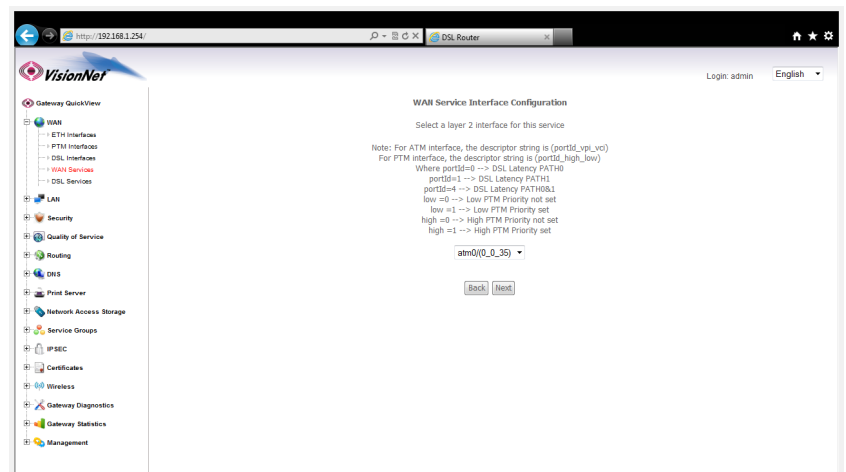
“Ethernet Services”



- 1.B Select **“Add”**



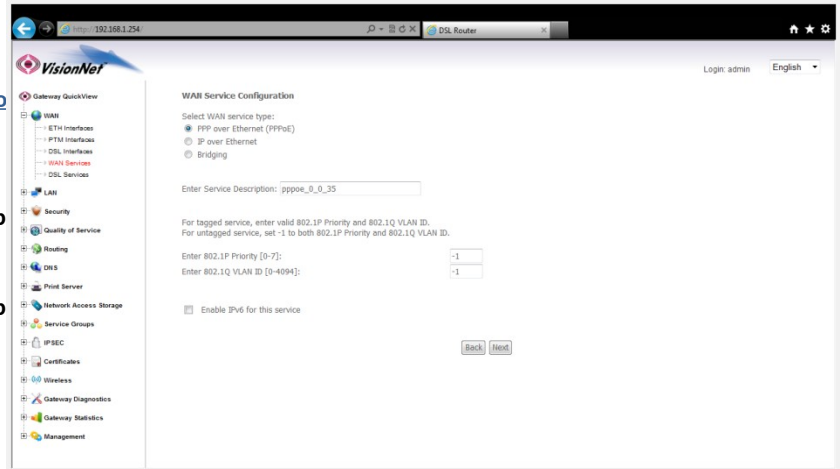
- 1.C Select the desired WAN Interface



Step 2: Configuring the WAN Service

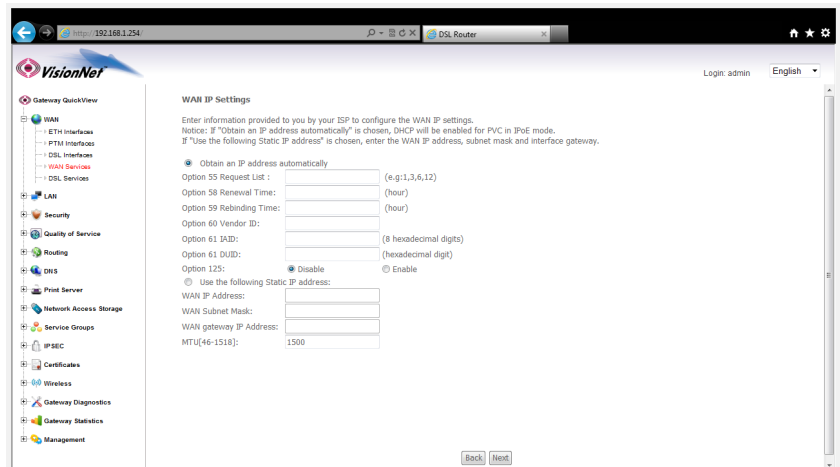
2.A WAN SERVICE CONFIGURATION.

Select WAN Service Type:	IPOE
Enter Service Description	Will not affect service - no spaces allowed
802.1P Tag (Only for VLAN Mux Services)	-1 Untagged Otherwise, choose appropriate tag
802.1Q Tag (Only for VLAN Mux Services)	-1 Untagged Otherwise, choose appropriate tag



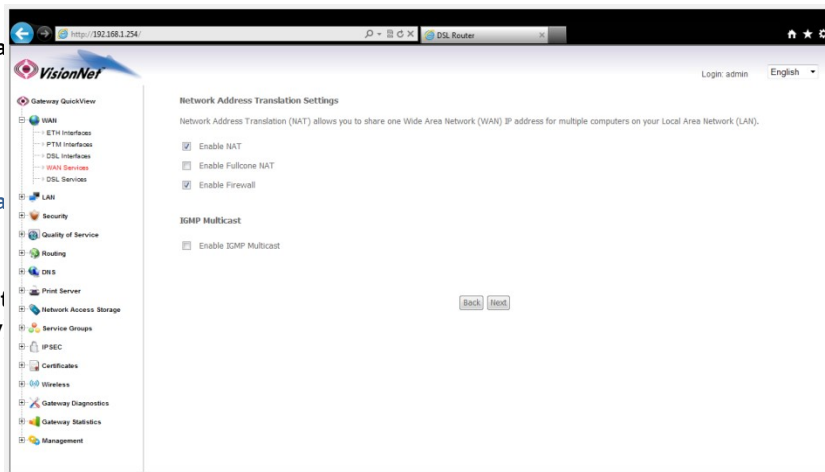
2.B Select "Next" and Proceed to "WAN IP Settings"

Obtain IP Address Automatically	For DHCP Service Only if specified by your Network Ops Manager
Options 55 to 61	Only if specified by your Network Ops Manager
Use the following Static IP	Enter appropriate information
MTU	1500 unless specified by your Network Operations Manager



2.C NAT and IGMP Multi Cast

Enable NAT	Enabled unless Public IPs are allocated to the LAN
Enable Full Cone NAT	Disabled
Enable Firewall	Enabled unless Public IPs are allocated to the LAN
IGMP Multi - Cast	Unless IGMP Multi Cast is used for IPTV (IGMP Proxy)



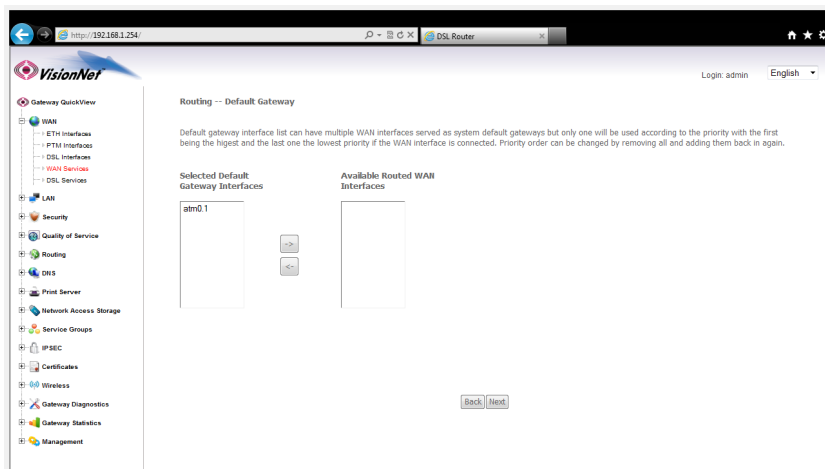
2.D Routing - Default Gateway

The DHCP Interface should be allocated to the "Selected Default Gateway" Interfaces.

This can be changed later.

The gateway priority is arranged from Top to Bottom

Gateways, that are not allocated, will not be used for the Routing Table

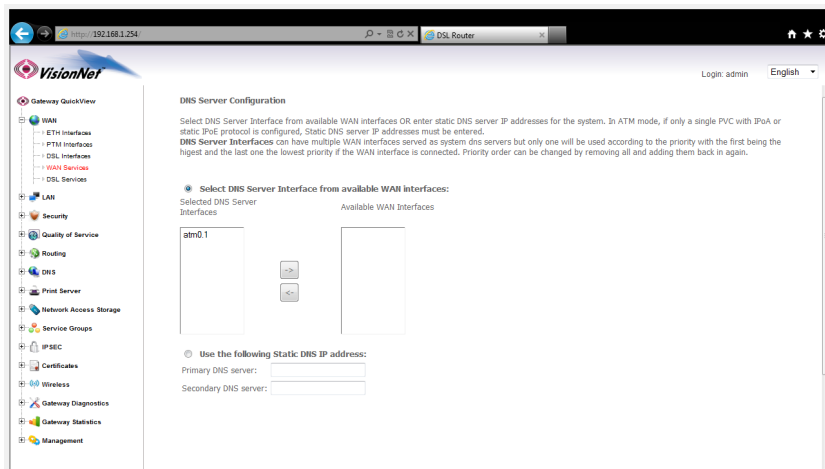


2.E DNS Server Configuration

You may prioritize the Dynamic DNS Servers

or

You may specify static DNS Servers



2.F When complete you may approve the settings. You will see the service populated in the "WAN Services" table

Section 3.8 – Creating a PPPoE WAN Service

Step 1: Selecting the WAN Service to Create

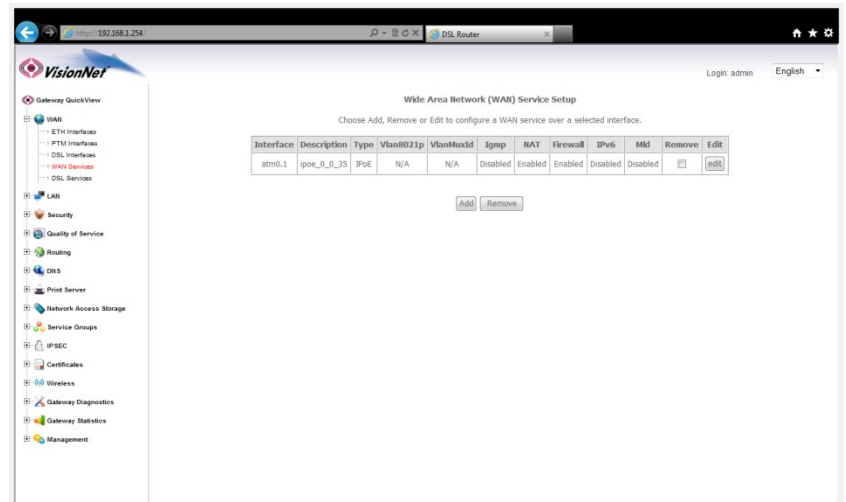
- 1.A Select the **“WAN”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select the appropriate WAN Interface

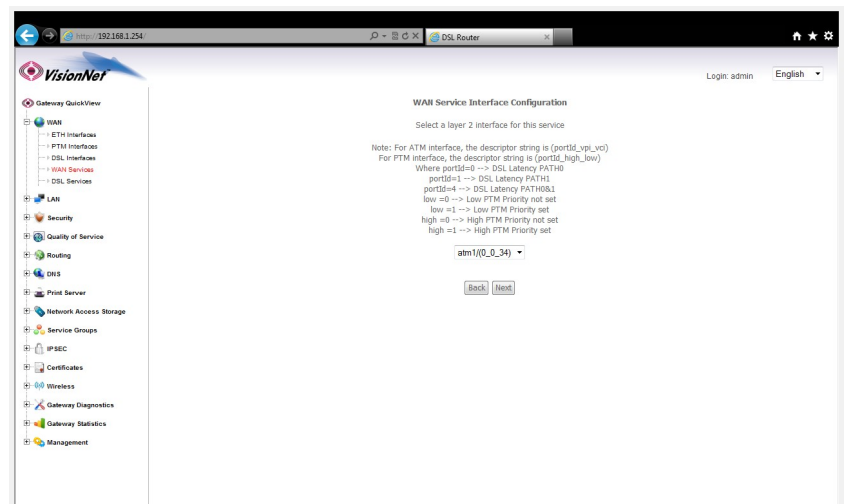
“Ethernet Services”



- 1.B Select **“Add”**



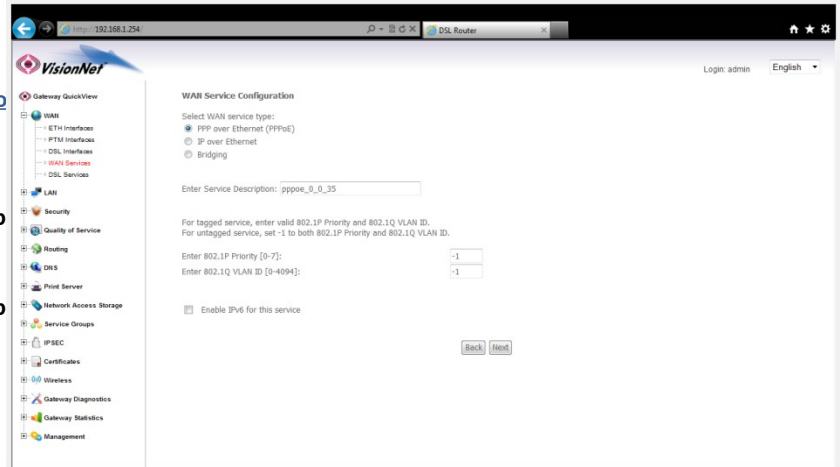
- 1.C Select the desired WAN Interface



Step 2: Configuring the WAN Service

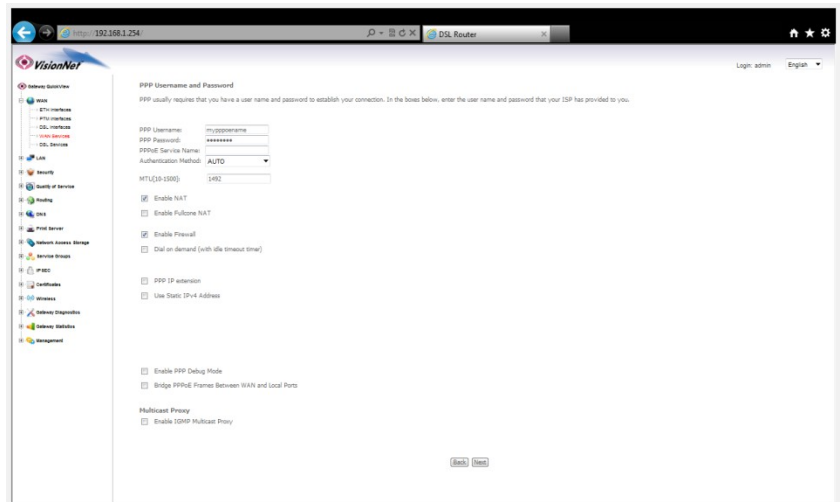
2.A WAN SERVICE CONFIGURATION.

Select WAN Service Type:	PPPoE
Enter Service Description	<u>Will not affect service - no spaces allowed</u>
802.1P Tag (Only for VLAN Mux Services)	<u>-1 Untagged</u> Otherwise, choose appropriate tag
802.1Q Tag (Only for VLAN Mux Services)	<u>-1 Untagged</u> Otherwise, choose appropriate tag



2.B Select “Next” and Proceed to “PPPoE Username and Password”

PPP Username	Enter unique Username
PPP Password	Enter unique Password
PPPoE Service Name	Leave blank unless specified by your Network Ops Manager
Authentication Method	AUTO unless specified by your Network Operations Manager
MTU	1492 unless specified by your Network Operations Manager
Enable NAT	Enabled, unless otherwise specified by Network Operations
Enable Full-Cone NAT	Disabled, unless specified otherwise by Network Operations
Dial on Demand	Disabled unless specified otherwise by Network Operations
PPPIP Extension	Disabled unless specified otherwise by Network Operations
Use Static IPv4 Address	Only use for static IP Settings
Enable PPP Debug Mode	Disabled - this is only for sending PPP packets to the Syslog for temporary troubleshooting
Bridge PPPoE Frames	Disabled - this will allow Clients to tunnel through the firewall to create a second PPPoE Session
MultiCast Proxy	Disabled unless specified otherwise by Network Operations



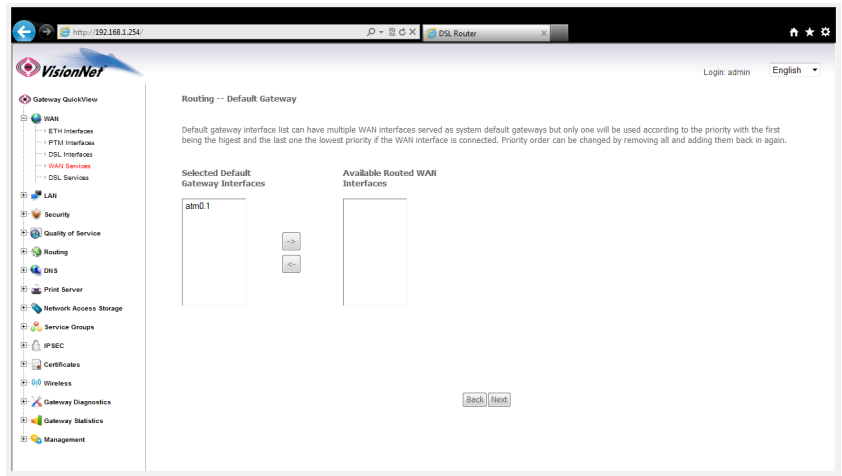
2.C Routing - Default Gateway

The DHCP Interface should be allocated to the “Selected Default Gateway” Interfaces.

This can be changed later.

The gateway priority is arranged from Top to Bottom

Gateways, that are not allocated, will not be used for the Routing Table

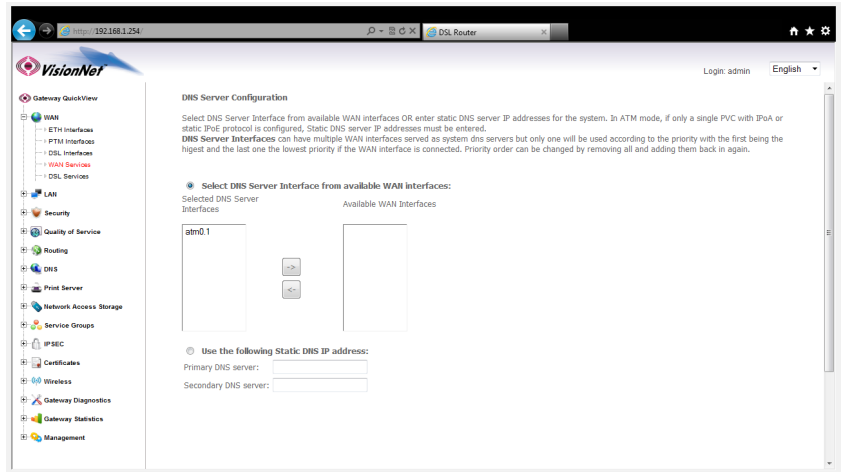


2.D DNS Server Configuration

You may prioritize the Dynamic DNS Servers

or

You may specify static DNS Servers



2.E When complete you may approve the settings. You will see the service populated in the “WAN Services” table

Section 3.9 – Creating a Bridge WAN Service

Step 1: Selecting the WAN Service to Create

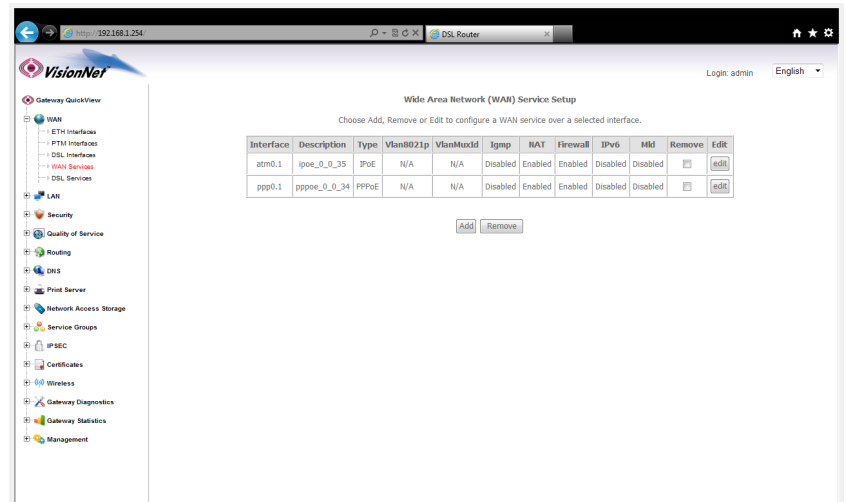
- 1.A Select the **“WAN”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select the appropriate WAN Interface

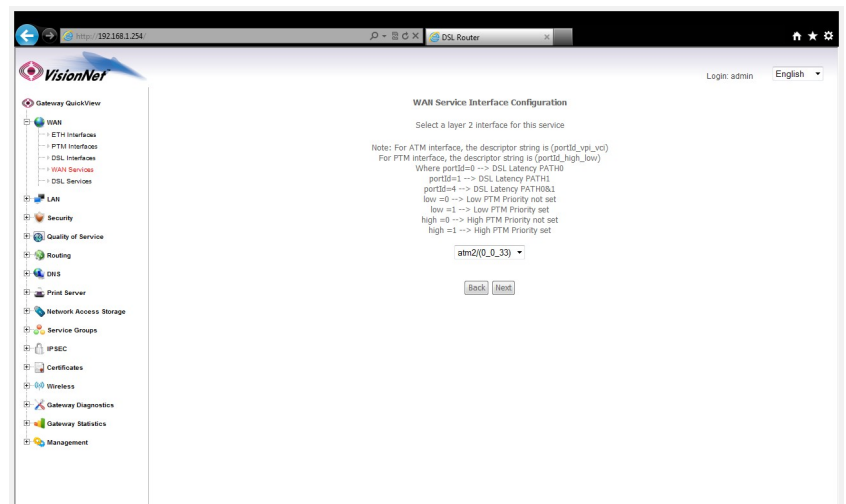
“Ethernet Services”



- 1.B Select **“Add”**



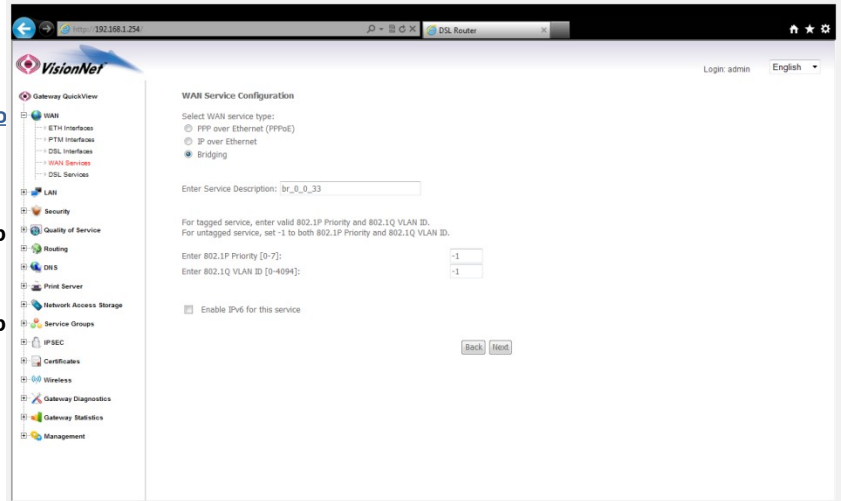
- 1.C Select the desired WAN Interface



Step 2: Configuring the WAN Service

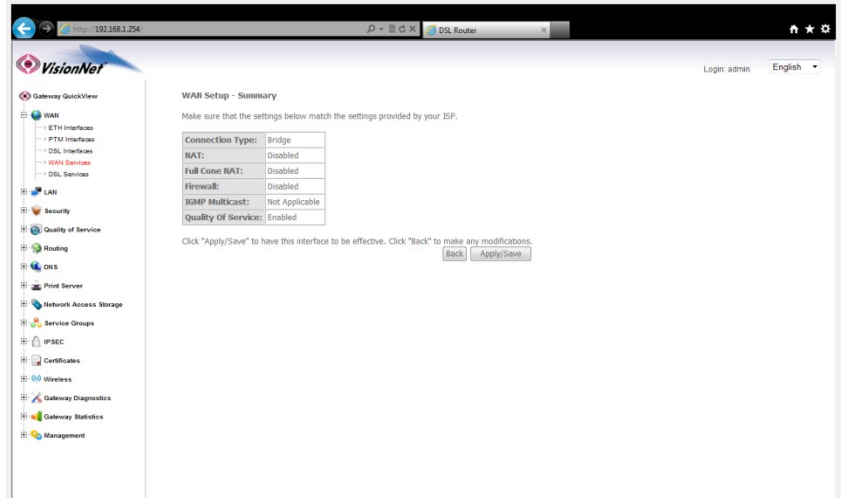
2.A WAN SERVICE CONFIGURATION.

Select WAN Service Type:	Bridging
Enter Service Description	<u>Will not affect service - no spaces allowed</u>
802.1P Tag (Only for VLAN Mux Services)	<u>-1 Untagged</u> Otherwise, choose appropriate tag
802.1Q Tag (Only for VLAN Mux Services)	<u>-1 Untagged</u> Otherwise, choose appropriate tag



2.B Select "Next" to complete the Bridge WAN Service

Select "Apply / Save"



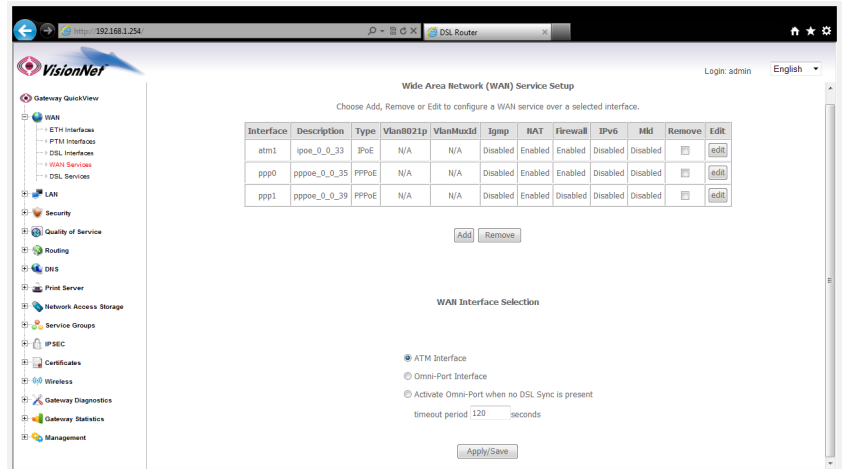
Section 3.10 – WAN Interface Prioritization

You may wish to support either the DSL or ATM Interface. You may choose the WAN Interface priority for your VisionNet gateway.

Step 1: Access the GUI to find the WAN Interface Page

- 1.A Select the **“WAN”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“WAN Services”**



- 1.B Select the appropriate setting under **“WAN INTERFACE SELECTION”**

ATM Interface	DSL ONLY
Omni-Port Interface	Ethernet ONL
Activate Omni-Port when no DSL Sync is present	DSL Primary, Ethernet Secondary
Timeout Period	Time, after be up, without C Sync prior to Ethernet Upli enabled

WAN Interface Selection

ATM Interface
 Omni-Port Interface
 Activate Omni-Port when no DSL Sync is present
 timeout period seconds

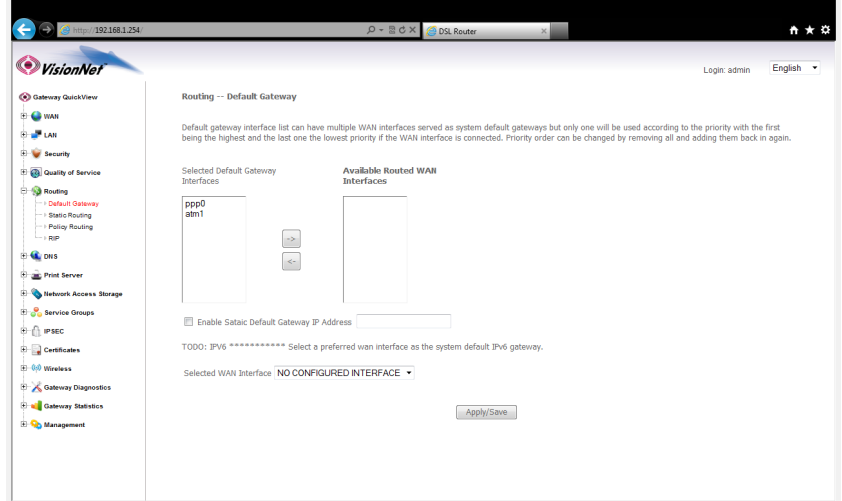
Section 3.11 - Gateway Prioritization

The VisionNet modem is designed to utilize each WAN specific gateway for it's intended purpose. You may specify which WAN Services are used for outbound traffic, and in which order, through Gateway Prioritization

Step 1: Access the GUI to find the Gateway Page

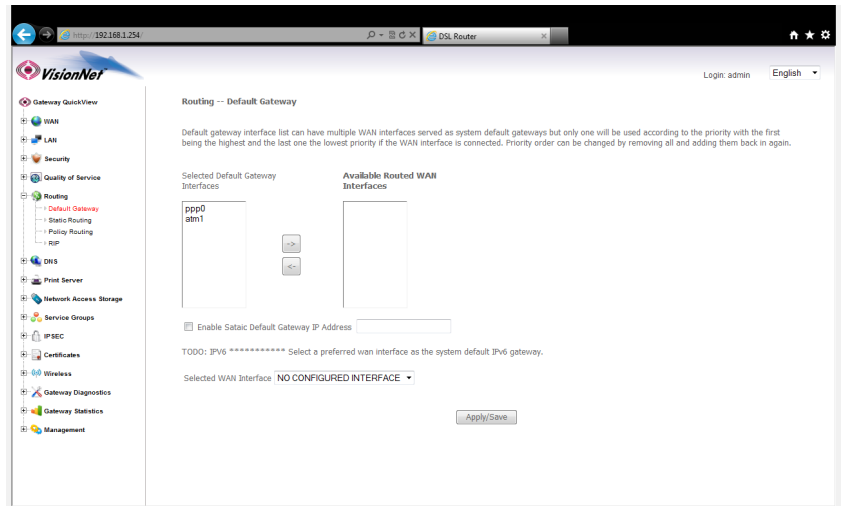
- 1.A Select the **"Routing"** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **"Default Gateway"**



- 1.B Check **"Select Default Gateway Interfaces"**

Gateways are prioritized from top to bottom



- 1.C Select **"Save"**

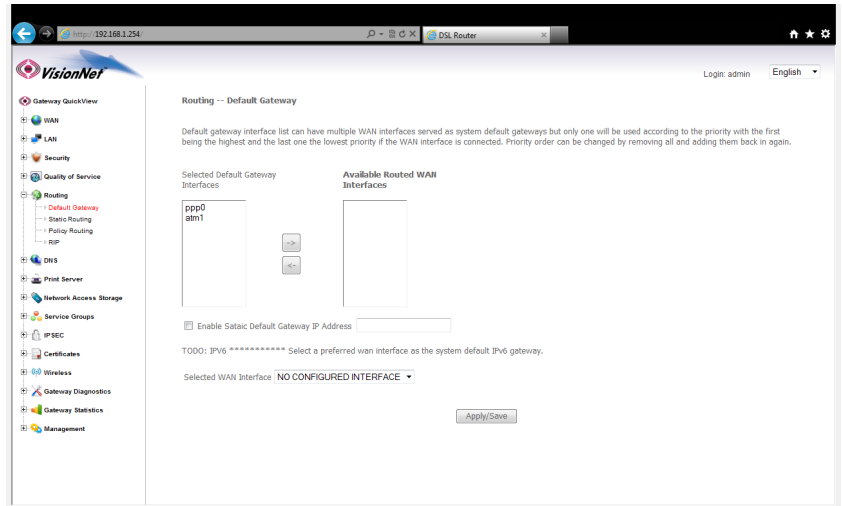
Section 3.12 – Universal Static Gateway Service

In the event that you would like to specify a universal gateway address, You may do so via the Gateway Prioritization Page

Step 1: Access the GUI to find the Gateway Page

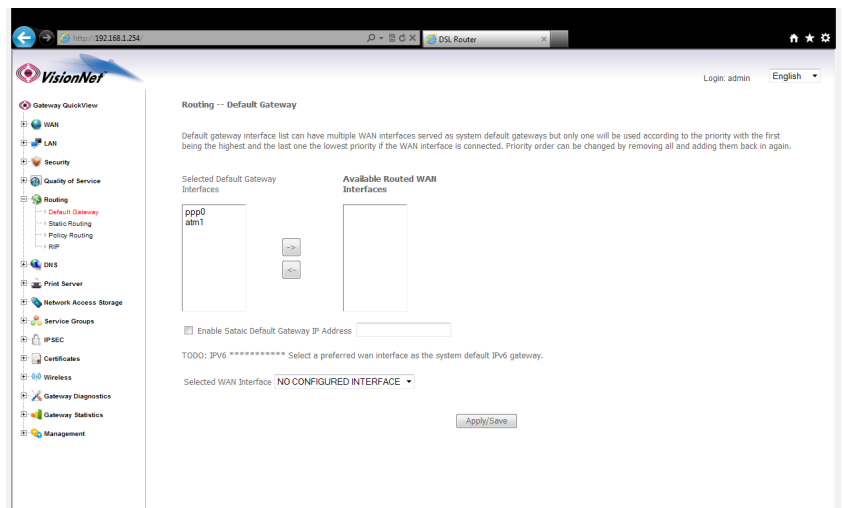
- 1.A Select the **“Routing”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“Default Gateway”**



- 1.B Check **“Enable Static Gateway IP Address”**

Enter the desired Static Gateway



- 1.C Select **“Save”**

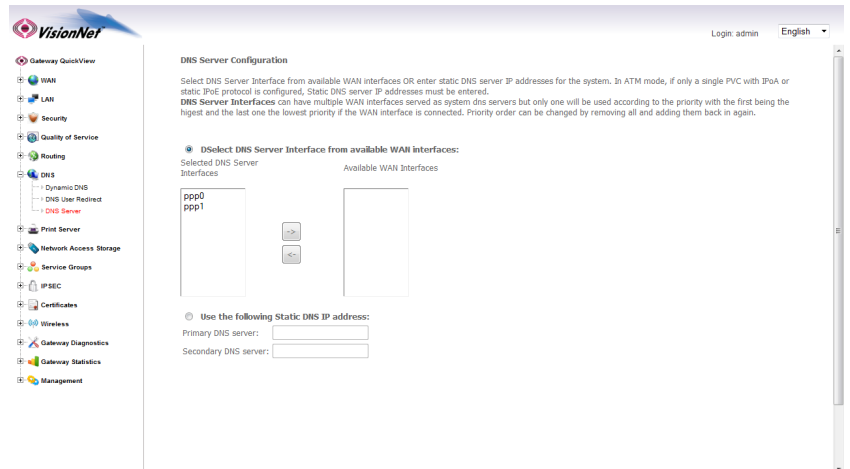
Section 3.13 – DNS Prioritization

You may use the DNS Server page to prioritize DNS Selection based upon WAN Services.

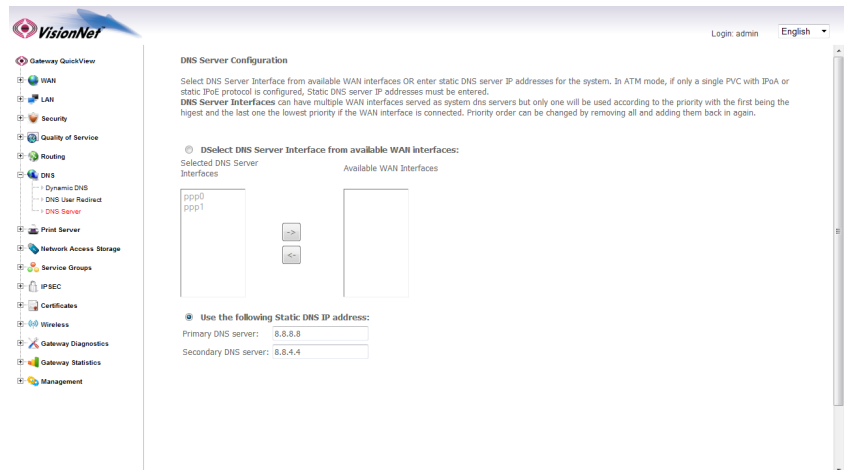
Step 1: Access the GUI to find the DNS Server Page

- 1.A Select the **“DNS”** tab located within the left-hand frameset.

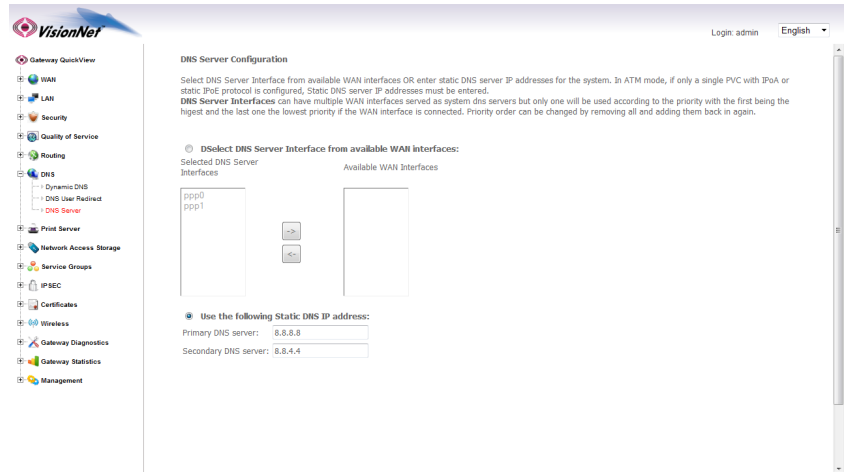
Then, in the left-hand frameset, select **“DNS Server”**



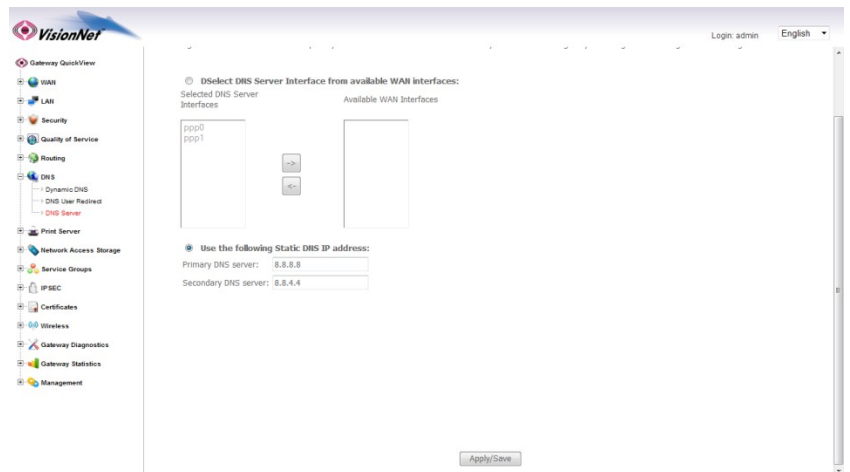
- 1.B Select **“Select DNS Server Interfaces from available WAN Interfaces”**



1.C Prioritize WAN Interfaces from Top to Bottom



1.D Select "Apply / Save" and then reboot the modem



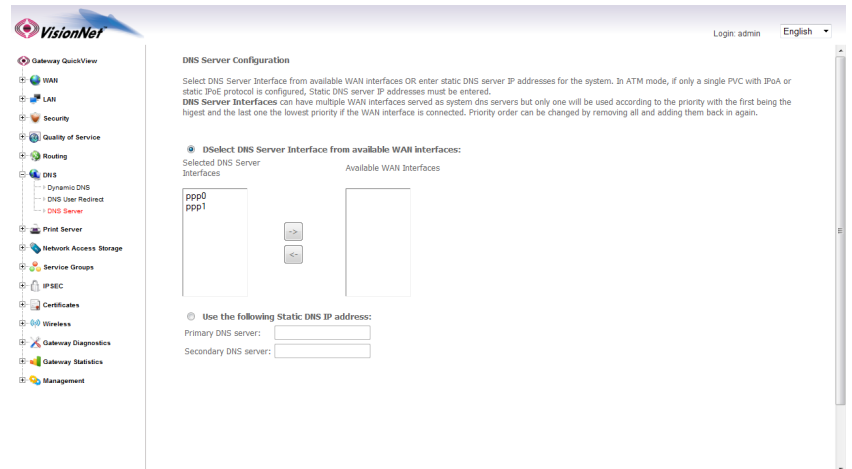
Section 3.14 – Universal Static DNS Addresses

The VisionNet Modem may be assigned different DNS addresses for each WAN Service. In the event that Static IPs are to be used, you may update and change the settings with the following procedure.

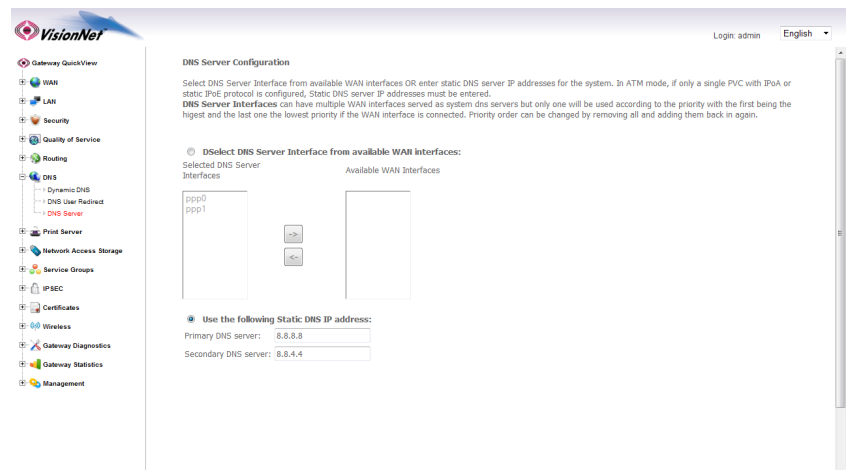
Step 1: Access the GUI to find the DNS Server Page

- 1.A Select the **“DNS”** tab located within the left-hand frameset.

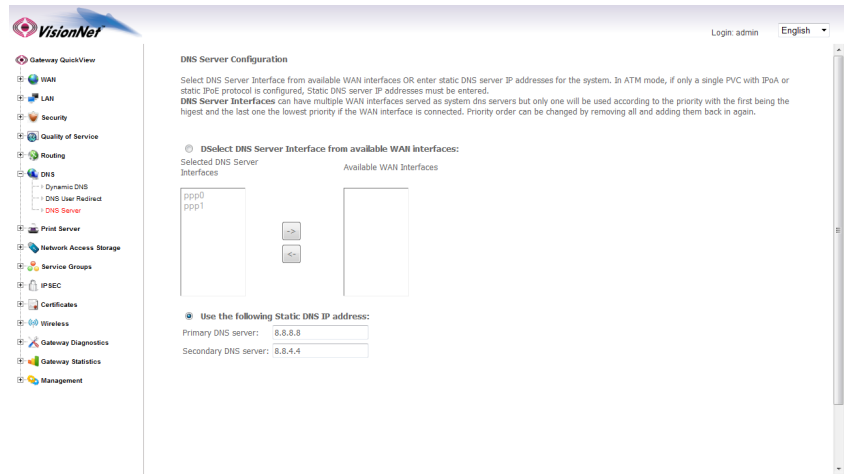
Then, in the left-hand frameset, select **“DNS Server”**



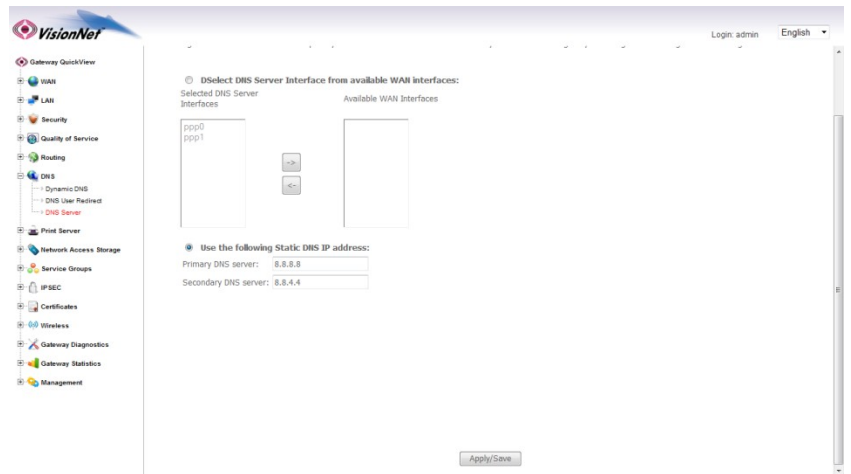
- 1.B Select **“Use the following Static DNS IP Address”**



1.C Enter the Primary and Secondary WAN DNS Addresses



1.D Select "Apply / Save" and then reboot the modem



SECTION 4: PUBLIC WAN IP ADDRESS ALLOCATION

Section 4.1 - Public IP Allocation – Public Subnet (WAN Interface within Subnet)

Prior to configuring the modem for a Public WAN Subnet, you must obtain the following information:

- 1) The WAN Subnet to be used: (ie: 172.16.100.9 /29)
- 2) The WAN Gateway to be used
- 3) The WAN DNS Addresses to be used

Designation	IP Address	Subnet
Network ID	172.20.111.144	255.255.255.248
Gateway WAN IP	172.20.111.145	255.255.255.248
Host B	172.20.111.146	255.255.255.248
Host C	172.20.111.147	255.255.255.248
Host D	172.20.111.148	255.255.255.248
Host E	172.20.111.149	255.255.255.248
Host F	172.20.111.150	255.255.255.248
Broadcast	172.20.111.151	255.255.255.248

Step 1: Select the appropriate WAN Service for modification

1.A Create the desired WAN Interface

Enter the required Public IP Information

The screenshot shows the VisionNet WAN IP Settings page. The left sidebar contains a navigation menu with options like Gateway QuickView, WAN, LAN, Security, Quality of Service, Routing, DNS, Print Server, Network Access Storage, Service Groups, IPSEC, Certificates, Wireless, Gateway Diagnostics, Gateway Statistics, and Management. The main content area is titled 'WAN IP Settings' and includes instructions: 'Enter information provided to you by your ISP to configure the WAN IP settings. Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in iPoE mode. If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.' There are two radio buttons: 'Obtain an IP address automatically' (selected) and 'Use the following Static IP address'. Below these are fields for Option 55 Request List, Option 58 Renewal Time, Option 59 Rebinding Time, Option 60 Vendor ID, Option 61 IAD, Option 61 DUID, and Option 125. The 'Use the following Static IP address' section is active, showing fields for WAN IP Address (172.20.100.146), WAN Subnet Mask (255.255.255.248), WAN gateway IP Address (172.20.100.145), and MTU(46-1518) (1500). 'Back' and 'Next' buttons are at the bottom right.

1.B Ensure the following settings

NAT must be DISABLED

Firewall must be DISABLED

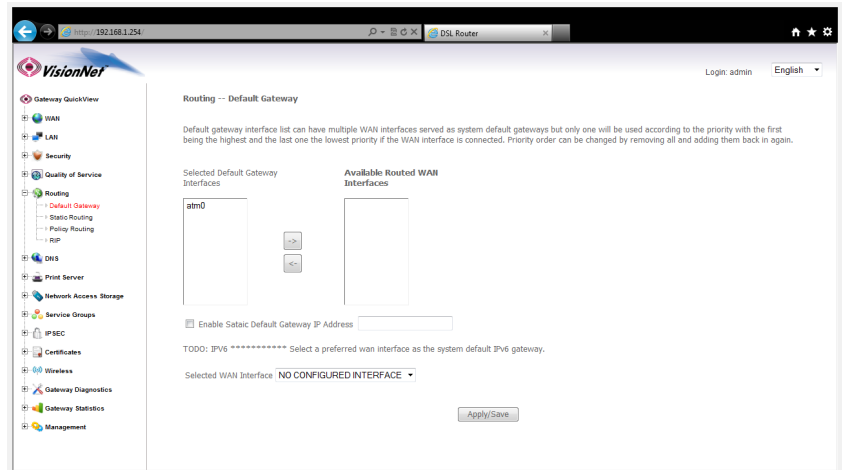
IGMP must be DISABLED

The screenshot shows the VisionNet Network Address Translation Settings page. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Network Address Translation Settings' and includes the text: 'Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN)'. There are three checkboxes: 'Enable NAT', 'Enable Firewall', and 'Enable IGMP Multicast'. All three are currently unchecked. 'Back' and 'Next' buttons are at the bottom right.

Step 2: Configure the Default Gateway

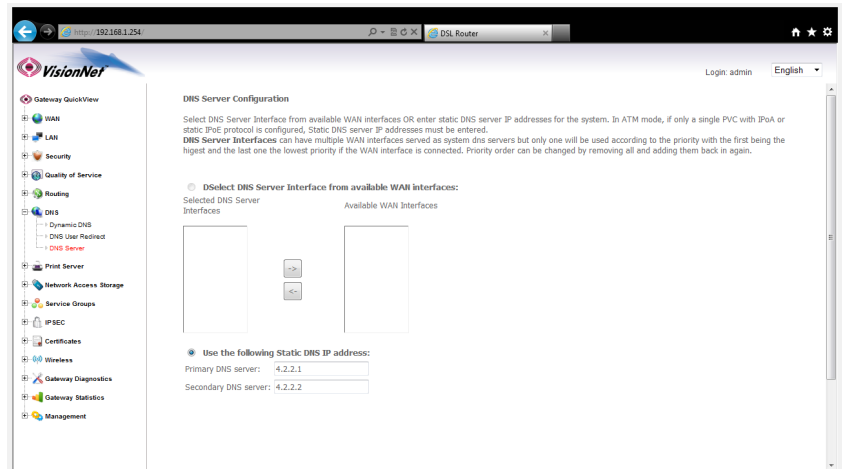
- 2.A You may need to specify the gateway interface if you are using a PPP connection. Select **“Routing”**

Enter ISP WAN Gateway



- 2.B You may also specify the static DNS Page by access **“DNS”** and then **“DNS SERVER”**

You may enter the Static DNS Information

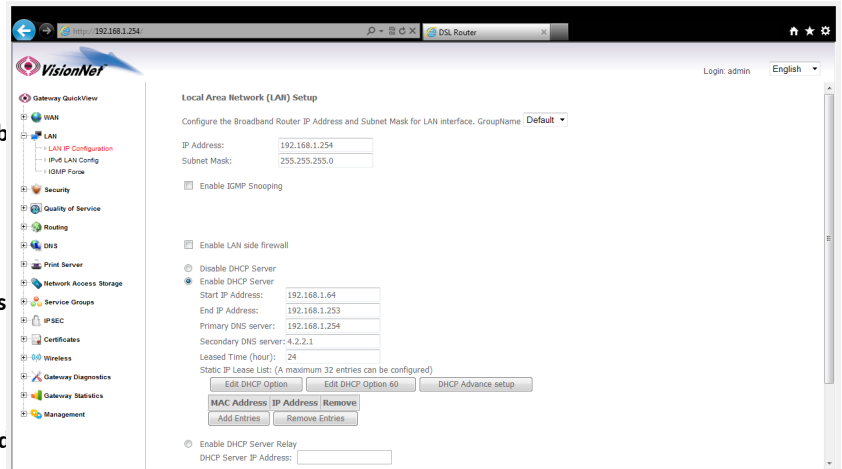


- 2.C Select **“Save / Apply”**

Step 3: Configure the LAN for Public IPs

3.A From the “LAN” page located in the left hand frameset under “[Advanced Setup](#)”

IP Address:	Same as the WAN IP Address
Subnet Mask:	255.255.255.248 (or appropriate)
Enable UPnP	Disabled
Enable IGMP Snooping:	Disabled
Enable LAN Side Firewall	Disabled
DHCP Server:	Enabled (Or Disabled depending)
Start IP Address:	Second Host IP Address
End IP Address:	6 th Host IP Address
Subnet Mask:	255.255.255.248
DNS Servers	Enter primary and Secondary
Leased Time (hour):	24
Reserve IP Address	Unnecessary
Configure Secondary IP Address:	Unchecked



3.B Once complete, select “Save/Reboot”











PLEASE NOTE THAT LAN DEVICES MUST BE REBOOT PRIOR TO OBTAINING NEW, PUBLIC, IP ADDRESSES

Section 4.2 – Public IP Allocation – Virtual Public Subnet (WAN Interface not within Subnet)

⚠ PLEASE NOTE: THIS IS ONLY FOR BUSINESS CUSTOMERS WHO HAVE BEEN ASSIGNED A SERIES OF STATIC IP ADDRESSES. PLEASE OBTAIN APPROVAL FROM A SUPPORT MANAGER BEFORE BEGINNING THIS PROCEDURE

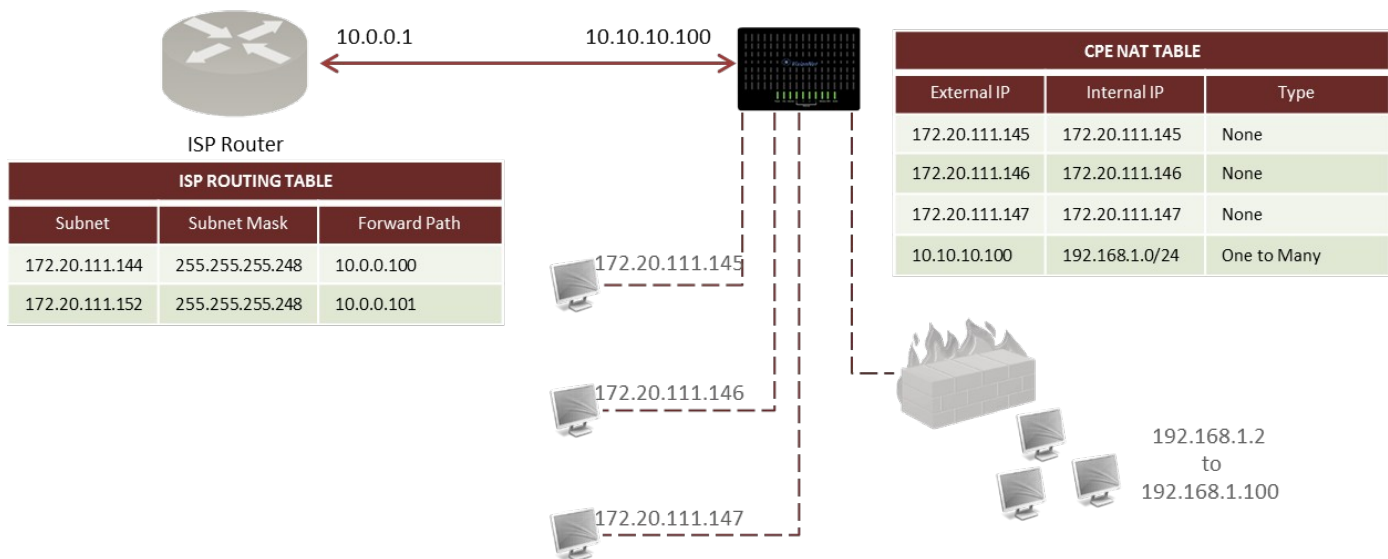
Prior to configuring the modem for a Public WAN Subnet, you must obtain the following information:

The WAN Subnet to be used: (ie: 172.16.100.144 /29)

Designation	IP Address	Subnet
Network ID 	172.20.111.144	255.255.255.248
Secondary LAN IP 	172.20.111.145	255.255.255.248
Host B 	172.20.111.146	255.255.255.248
Host C 	172.20.111.147	255.255.255.248
Host D 	172.20.111.148	255.255.255.248
Host E 	172.20.111.149	255.255.255.248
Host F 	172.20.111.150	255.255.255.248
Broadcast 	172.20.111.151	255.255.255.248

Why Virtual IP Allocation

You may wish to allocate IP Addresses, directly to devices, that are assigned to the customer; but not the primary WAN Interface of the Gateway



Step 1: Edit an existing WAN Connection

1.A In the left-hand frameset select “WAN”

The screenshot shows the VisionNet Gateway QuickView interface. On the left, a navigation tree is expanded to 'WAN'. The main area displays the 'Wide Area Network (WAN) Service Setup' page. Below the heading, there is a table with columns: Interface, Description, Type, Vlan8021p, VlanMuxId, Igmp, NAT, Firewall, IPv6, Mfd, Remove, and Edit. Two rows are visible: 'ppp0' and 'ppp1'. The 'NAT' column for both rows has a checked checkbox. Below the table are 'Add' and 'Remove' buttons.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mfd	Remove	Edit
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	edit
ppp1	pppoe_0_0_34	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	edit

Then select “WAN Services”

1.B

Choose the appropriate WAN Service, and select “Edit”

This screenshot is identical to the previous one, but the 'Edit' link in the 'ppp1' row of the table is highlighted in red, indicating it has been selected.

1.C

Disable “Firewall”
ONLY “ENABLE NAT” SHOULD BE ENABLED!!!

The screenshot shows the 'PPP Username and Password' configuration page. It includes fields for PPP Username (XXXXXXXX@mybrch.net), PPP Password (masked with asterisks), PPPoE Service Name, Authentication Method (set to AUTO), and MTU[10-1500] (set to 1492). There are several checkboxes: 'Enable NAT' (checked), 'Enable Fullcone NAT' (unchecked), 'Enable Firewall' (unchecked), 'Dial on demand (with idle timeout timer)' (unchecked), 'PPP IP extension' (unchecked), and 'Use Static IPv4 Address' (unchecked).

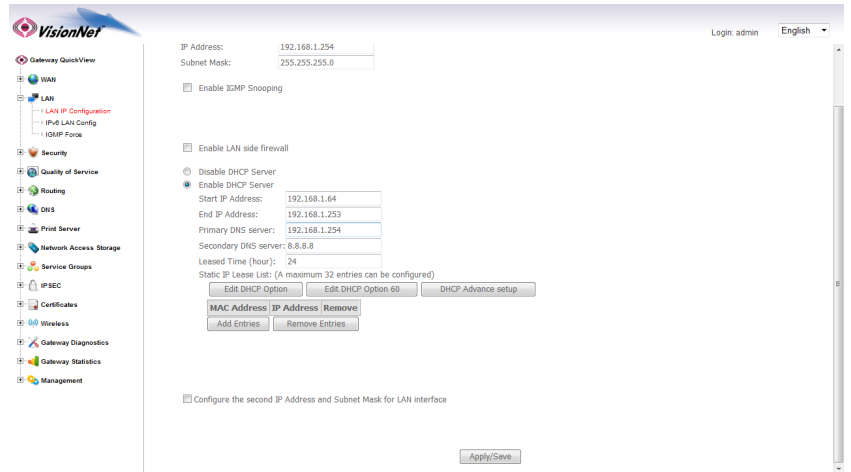
1.D Review the WAN Setup Summary

Select "Apply / Save"



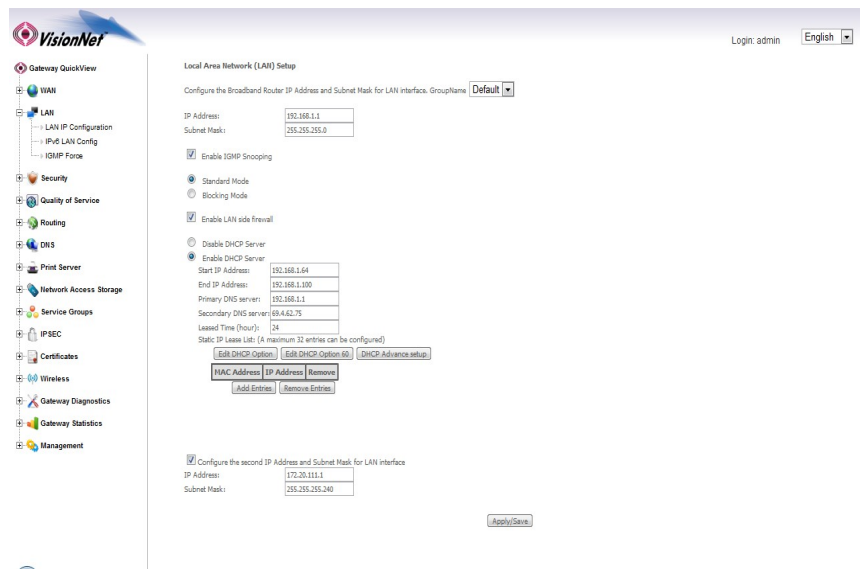
Step 2: Direct Your Browser to the LAN Configuration Page

2.A Select the "LAN" tab located within the left-hand frameset.



Then, in the left-hand frameset, select "LAN IP Configuration"

2.B Select [Configure the Second IP Address and Subnet Mask for LAN Interface](#)



Enter the first usable Host within the desired subnet

Enter the Subnet Mask (255.255.255.248)

2.C Select "Apply Save"

Step 3: Configure Hosts

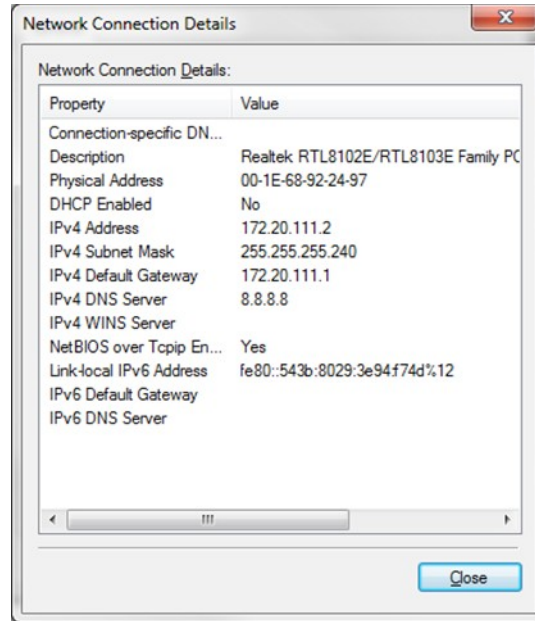
3.A EACH HOST MUST BE CONFIGURED WITH THE FOLLOWING SETTING

IP ADDRESS: Usable Host

Subnet Mask: 255.255.255.248

**Gateway: First Usable Host (CPE
LAN IP Address)**









**DNS Address: Choose appropriate
Birch DNS Servers**



Section 4.3 - Public IP Allocation – 1:1 NAT Public Subnet

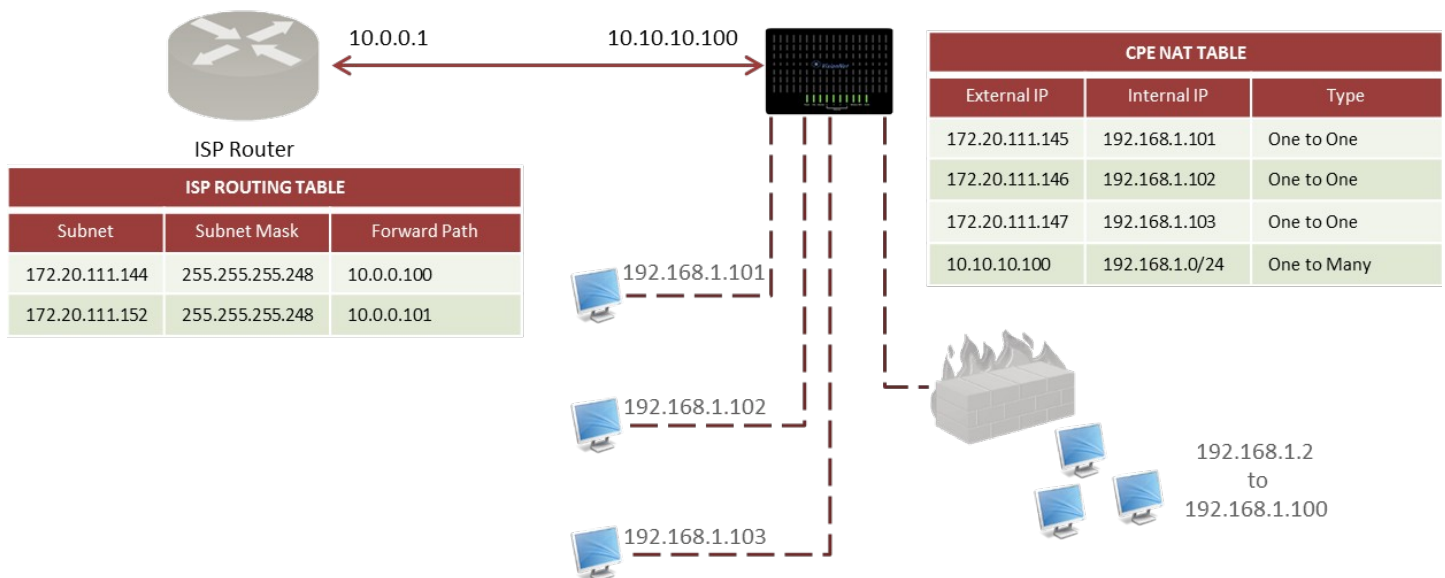
Prior to configuring the modem for a Public WAN Subnet, you must obtain the following information:

- 1) **The WAN Subnet to be used: (ie: 172.16.100.144 /29)**
- 2) **The WAN Gateway to be used**
- 3) **The WAN DNS Addresses to be used**

Designation		IP Address	Subnet
Network ID		172.20.111.144	255.255.255.248
Host A		172.20.111.145	255.255.255.248
Host B		172.20.111.146	255.255.255.248
Host C		172.20.111.147	255.255.255.248
Host D		172.20.111.148	255.255.255.248
Host E		172.20.111.149	255.255.255.248
Host F		172.20.111.150	255.255.255.248
Broadcast		172.20.111.151	255.255.255.248

Why 1:1 NAT (Multi-NAT)

Multi-NAT will allow you to forward traffic, destined for a WAN IP Address within the assigned subnet, to an internal Host assigned with a private LAN IP.



Step 1: Edit an existing WAN Connection

1.A In the left-hand frameset select “WAN”

The screenshot shows the VisionNet Gateway QuickView interface. On the left, a navigation tree is expanded to 'WAN Services'. The main content area is titled 'Wide Area Network (WAN) Service Setup' and contains a table with the following data:

Interface	Description	Type	Vlan8021p	VlanMuxId	Icmp	NAT	Firewall	IPv6	Md	Remove	Edit
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	edit
ppp1	pppoe_0_0_34	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	edit

Below the table are 'Add' and 'Remove' buttons.

Then select “WAN Services”

1.B

Choose the appropriate WAN Service, and select “Edit”

This screenshot is identical to the previous one, but the 'edit' button in the second row of the table is highlighted with a red box, indicating the selection of the 'ppp1' service for editing.

1.C

Disable “Firewall”

ONLY “ENABLE NAT” SHOULD BE ENABLED!!!

The screenshot shows the 'PPP Username and Password' configuration page. The 'Authentication Method' is set to 'AUTO'. The 'Enable Firewall' checkbox is unchecked, while the 'Enable NAT' checkbox is checked.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

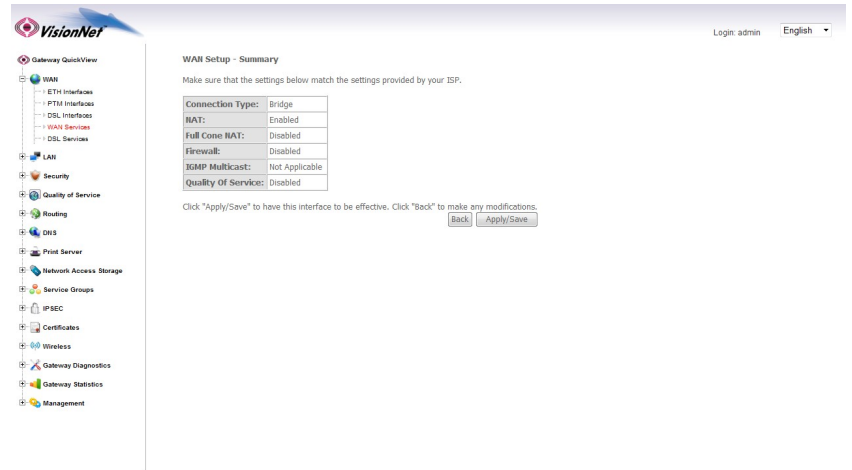
PPP Username: XXXXXXXXXXX@mybird.net
 PPP Password: *****
 PPPoE Service Name:
 Authentication Method: AUTO
 MTU(10-1500): 1492

Enable NAT
 Enable Fullcone NAT
 Enable Firewall
 Dial on demand (with idle timeout timer)

PPP IP extension
 Use Static IPv4 Address

1.D Review the WAN Setup Summary

Select “Apply / Save”



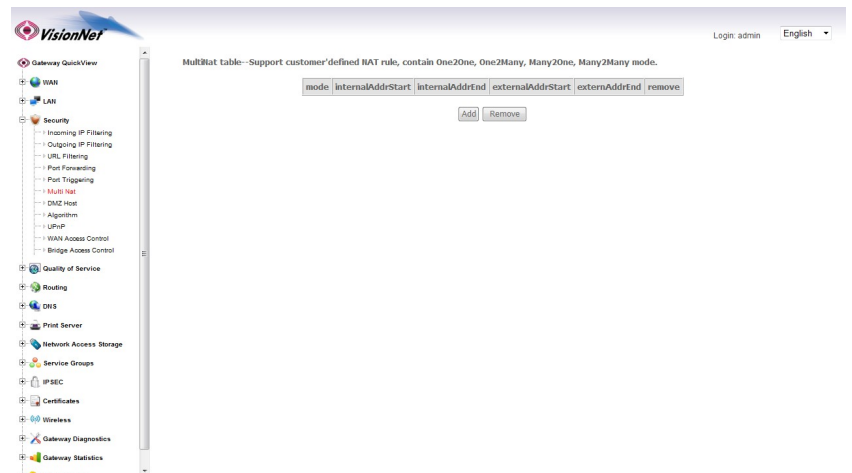
Step 2: Apply Static LAN IPs to Devices to that will have direct WAN Access

2.A Please see section 4.2 for further instruction

Step 3: Configure 1:1 NAT

3.A In the left-hand frameset select “Security”

Then select “Multi-NAT”



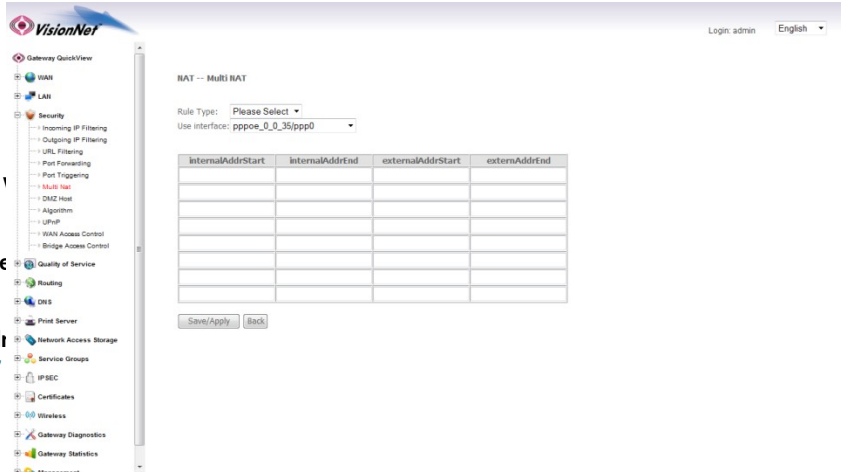
3.B Select Add

Rule Type: One to One

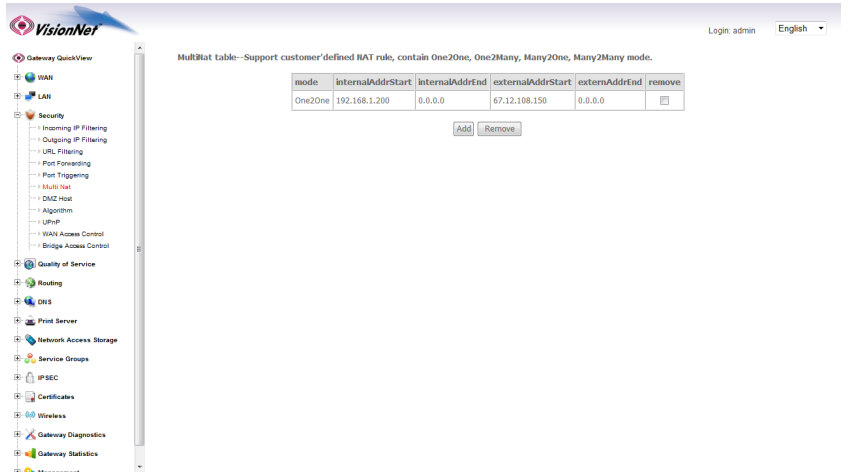
Use Interface: Choose appropriate Interface

Internal AddrStart: Choose LAN IP Address - ie: 192.168.1.200

External AddrStart: Choose WAN IP Address - ie: 172.20.111.147



3.C Review the NAT Table



Section 4.4 - Public IP Allocation – PPPoE Extension

Why PPPoE Extension?

- You may wish for the modem to manage the PPP Authentication
- You may wish for the IP Address, obtained by the Gateway, to forward to a LAN Host
- You may not wish for a full subnet to be assigned

PPPoE Extension will forward the Gateway's WAN IP to the first LAN Host that makes a DHCP request

Step 1: When creating a WAN Connection

1.A PPP Configuration

PPPoE Extension must be enabled

The screenshot shows the 'PPP Username and Password' configuration page in the VisionNet web interface. The page title is 'PPP Username and Password'. Below the title, there is a note: 'PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.' The configuration fields are as follows:

- PPP Username: mypppusername
- PPP Password: *****
- PPP Service Name: [empty]
- Authentication Method: AUTO
- MTU(0-1500): 1492

Below these fields, there are several checkboxes:

- Enable NAT
- Enable Fullcone NAT
- Enable Firewall
- Dial on Demand (with idle timeout time)
- PPP IP extension
- Use Static IPv4 address
- Enable PPP Debug Mode
- Bridge PPPoE Frames Between WAN and Local Ports

At the bottom, there is a 'Multicast Proxy' section with a checkbox for 'Enable IGMP Multicast Proxy' which is unchecked. 'Back' and 'Next' buttons are located at the bottom right of the configuration area.

1.B NAT must be DISABLED

Full Cone NAT must be DISABLED

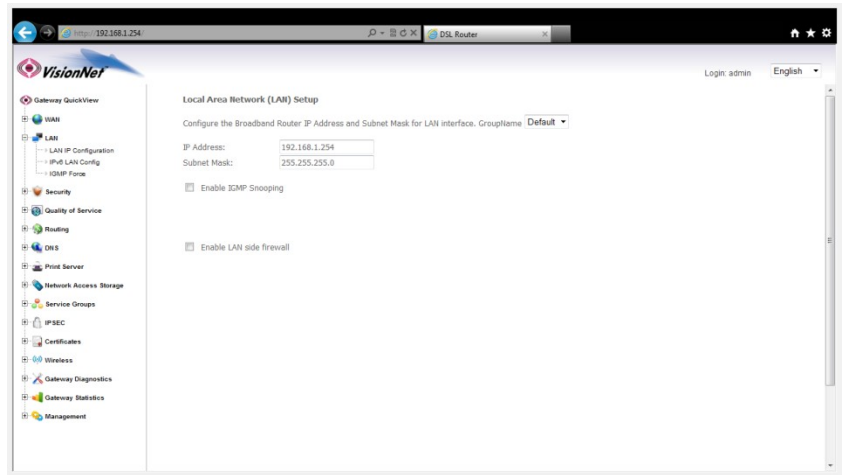
Firewall must be DISABLED

The screenshot shows the 'WAN Setup - Summary' page in the VisionNet web interface. The page title is 'WAN Setup - Summary'. Below the title, there is a note: 'Make sure that the settings below match the settings provided by your ISP.' The configuration is summarized in the following table:

Connection Type:	Bridge
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality of Service:	Disabled

Below the table, there is a note: 'Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.' At the bottom right, there are 'Back' and 'Apply/Save' buttons.

1.C The LAN Section will be modified automatically



SECTION 5: LAN CONFIGURATION

Section 5.1 – Configuration LAN Services

Step 1: Direct Your Browser to the LAN Configuration Page

- 1.A Select the **“LAN”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“LAN IP CONFIGURATION”**

The screenshot shows the VisionNet web interface. On the left, a navigation tree is visible with 'LAN IP Configuration' selected. The main content area is titled 'Local Area Network (LAN) Setup'. It includes a dropdown for 'Group Name' set to 'Default'. Below this are input fields for 'IP Address' (192.168.1.254) and 'Subnet Mask' (255.255.255.0). There are several checkboxes: 'Enable IGMP Snooping' (unchecked), 'Enable LAN side firewall' (unchecked), and 'Enable DHCP Server' (checked). Under 'Enable DHCP Server', there are fields for 'Start IP Address' (192.168.1.64), 'End IP Address' (192.168.1.253), 'Primary DNS server' (0.0.0.0), and 'Secondary DNS server' (0.0.0.0). A 'Leased Time (hour)' field is set to 24. Below these are buttons for 'Edit DHCP Option', 'Edit DHCP Option 60', and 'DHCP Advance setup'. At the bottom, there are sections for 'MAC Address', 'IP Address', and 'Remove' with 'Add Entries' and 'Remove Entries' buttons. A checkbox at the very bottom is labeled 'Configure the second IP Address and Subnet Mask for LAN interface'.

Step 2: Configure LAN Settings

- 2.A Configure the LAN IP Characteristics

IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Enable IGMP Snooping:	Unchecked
DHCP Server:	Enabled
Start IP Address:	192.168.1.64
End IP Address:	192.168.1.100
Primary DNS Server:	192.168.1.254
Secondary DNS Server:	WAN DNS Ad
Leased Time (hour):	24
All other settings	Unnecessary
Configure Second IP Address:	Unchecked

This screenshot is similar to the one above, but it shows the 'Apply/Save' button at the bottom right of the configuration page. The configuration values are consistent with the table provided.

- 2.B Select **“Apply / Save”**

Section 5.2 – Reserving an IP Address Within the DHCP Server

DEFINITION OF RESERVED IP

Some applications (Such as Port Triggering and DMZ Host) require a Static IP Address. Some devices, however, do not support Static IP Addresses or are portable in nature.

These devices may be provided a Static IP Address via the DHCP Server. When a Reserved IP Address is specified, the modem will consistently provide the same dynamic IP Address to the specified MAC Address. The Reserved IP Address will not be assigned to any other LAN Devices.

Prior to Assigning the Reserved IP Address, you must determine the MAC Address of the target LAN Device. You may copy the MAC Address from the ARP Table located within the Device Info Section of the GUI.

Step 1: Direct Your Browser to the LAN Configuration Page

- 1.A Select the **“LAN”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“LAN IP Configuration”**

The screenshot shows the VisionNet Gateway QuickView interface. The left-hand navigation pane is expanded to the LAN section, with 'LAN IP Configuration' selected. The main content area is titled 'DHCP Static IP Lease' and contains the following fields and controls:

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0
- Enable IGMP Snooping
- Enable LAN side firewall
- Disable DHCP Server
- Enable DHCP Server
- Start IP Address: 192.168.1.64
- End IP Address: 192.168.1.253
- Primary DNS server: 192.168.1.254
- Secondary DNS server: 8.8.8.8
- Leased Time (hour): 24
- Static IP Lease List: (A maximum 32 entries can be configured)
- Buttons: Edit DHCP Option, Edit DHCP Option 60, DHCP Advance setup
- Table headers: MAC Address, IP Address, Remove
- Buttons: Add Entries, Remove Entries
- Configure the second IP Address and Subnet Mask for LAN interface
- Apply/Save button

- 1.B Select **“Add Entries”**

You will be re-directed to the **“DHCP Static IP Lease”** Page

Enter the MAC Address of the intended LAN Host, and the IP Address that you would like to permanently allocate to that host.

The screenshot shows the VisionNet Gateway QuickView interface. The left-hand navigation pane is expanded to the LAN section, with 'LAN IP Configuration' selected. The main content area is titled 'DHCP Static IP Lease' and contains the following fields and controls:

- Enter the Mac address and Static IP address then click Apply/Save .
- MAC Address: 11:22:33-AA-BB-CC
- IP Address: 192.168.1.201
- Apply/Save button

- 1.C Select **“Apply Save”**

Section 5.3 – IGMP Force

IGMP Rules

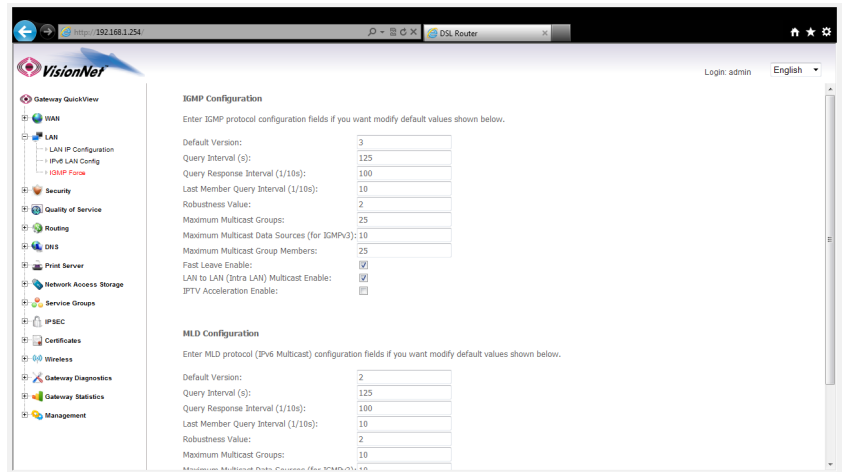
When IGMP Proxy is used, you may force the IGMP values and conventions.

There are times that you may wish to define one protocol exclusively (IE IGMP v3 in lieu of v2)

Step 1: Direct Your Browser to the LAN Configuration Page

- 1.A Select the **“LAN”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“IGMP Force”**



- 1.B Make desired changes

- 1.C Select **“Apply Save”**

SECTION 6: SECURITY CONFIGURATION

Section 6.1 – Port Forwarding

VISIONNET MODEMS ARE PRE-CONFIGURED FOR THE FOLLOWING APPLICATIONS:

XBOX:

UPnP will resolve most XBOX issues, however should you need to do further trouble-shooting the following Port Forwarding Rules may be enabled

Designation	WAN Port	LAN IP	LAN Port	Protocol
XBOX Live	88	192.168.1.230	88	TCP/UDP
XBOX Live	3074	192.168.1.230	3074	TCP/UDP

The most effective method of utilizing these rules, is to request that the end-user change the IP Address of their XBOX to the following Static IP settings:

XBOX Configuration	
IP Address	192.168.1.230
Subnet Mask	255.255.255.0
Gateway Address	192.168.1.254
DNS Address	192.168.1.254

IP CAMERAS:

IP Camera Port Forwarding Rules have been enabled

Designation	WAN Port	LAN IP	LAN Port	Protocol
Camera 1	6231	192.168.1.231	80	TCP/UDP
Camera 2	6232	192.168.1.232	80	TCP/UDP
Camera 3	6233	192.168.1.233	80	TCP/UDP
Camera 4	6234	192.168.1.234	80	TCP/UDP

The most effective method of utilizing these rules, is to request that the end-user change the IP Address of their Camera to the following Static IP settings:

IP Camera Configuration	
IP Address	192.168.1.23x
Subnet Mask	255.255.255.0
Gateway Address	192.168.1.254
DNS Address	192.168.1.254

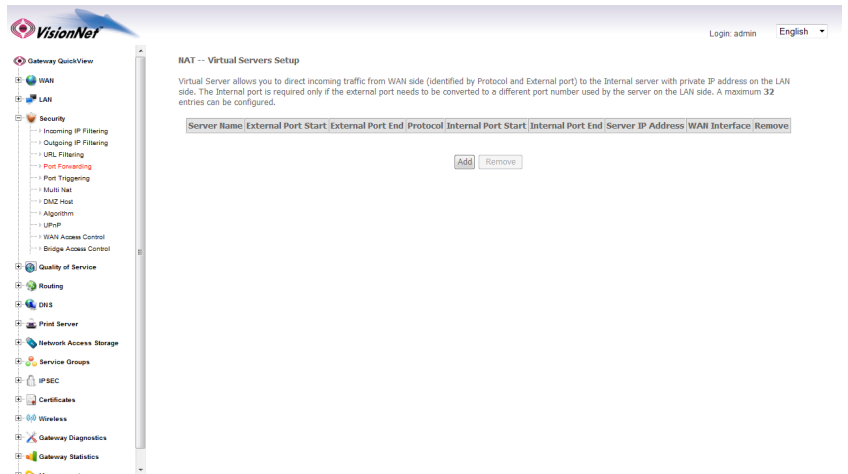
The customer will remotely access their camera by pointing their browser to the Public IP Address of the modem, and appending the appropriate port number. (ie: 67.126.108.104:6231)

The customer should have either a static IP, or a DynDNS URL Account to ensure that they may access the camera consistently. The customer can configure DynDNS settings via the end-user login.


Step 1: Direct Your Browser to the Port Forwarding Configuration Page

- 1.A Select the **“Security”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“Port Forwarding”**



- 1.B Select the **“Add”** Button.

 **Please Note: If the port to be assigned is already specified in the existing Port Forwarding Table, you must remove the rule containing this port prior to creating a new one.**

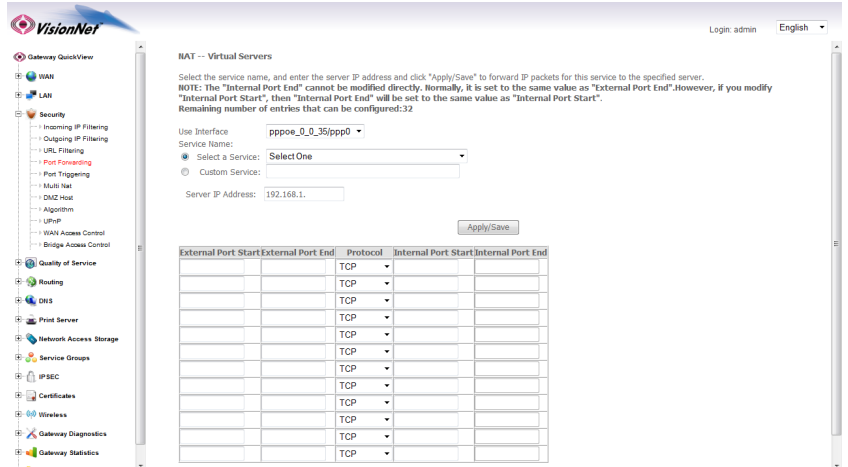
Step 2: Configure the Port Forwarding Rule

2.A Choose the name of the rule

Choose the appropriate WAN Interface:

If the Service you would like to have is already available in the [“Select a Service”](#) menu, you may select this service for auto-population.

You may create a custom Service by selecting [“Custom Service”](#) and entering a new rule name



2.B Enter the port rules

External Port Start This is the port that will be used to access the device on the WAN Side

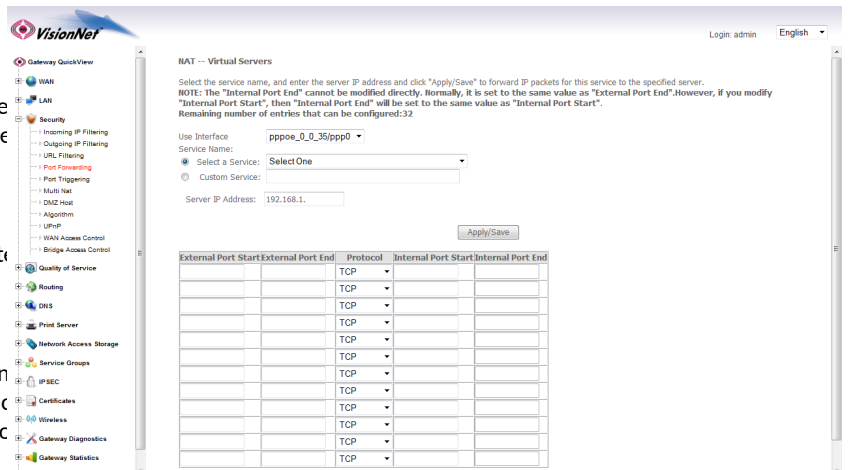
External Port End This should be the same as “External Port Start”

Protocol This should be “TCP/UDP” to avoid possible errors due to end-user miscommunication

Internal Port Start This should be the port that the device “listens” on (see IP Came example)

External Port End This should be the same as “Internal Port Start”

Remote IP This should left blank, unless on one remote device, with a static will be allowed to access this pc



2.C Select [“Save/Apply”](#)

2.D Considerations

For this rule to work properly, the LAN device must have either a Static IP, or a Reserved IP

The LAN Device, and modem, may should be reset to ensure that this rule continues to work correctly

Section 6.2 – Port Triggering

DEFINITION OF PORT TRIGGERING

Port Triggering is a dynamic version of Port Forwarding, in which the modem will dynamically create a temporary port forwarding rule based upon outbound activity. This is best applied for LAN devices that communicate with a remote server. Basic VPN functions are already supported by default, but some applications use non-standard communication methods.

An example would be port triggering configuration for the Nortel Contivity VPN Solution, which uses non-standard port VPN ports and requires Port Triggering to work.

The following are the port triggering rules required for Nortel Contivity VPNs.

Port Triggering for Nortel Contivity VPNs	LAN Device	Outbound	Port Temporarily Forwarded to	Inbound
	Outbound Port	Protocol	Initiating LAN Device	Protocol
	500	TCP/UDP	500	TCP/UDP
	10001	TCP/UDP	10001	TCP/UDP

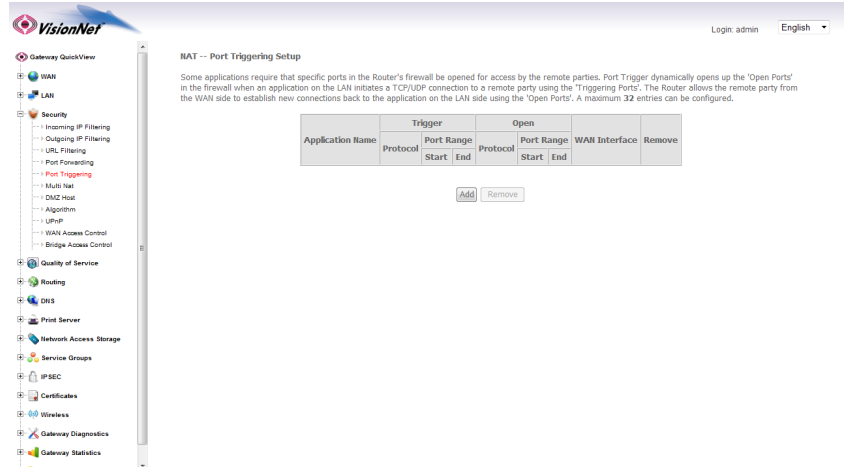
In this scenario, a LAN Device (ie: The end-user's laptop) will make an outbound UDP request on ports 500 and 10001. The modem responds to this by temporarily forwarding ports 500 and 10001 to the IP address of the initiating LAN Device (ie: The end-user's laptop) for the life of the session.

Port Triggering is ideal for portable devices (ie: laptops, PDAs, etc) which require port forwarding, but for which a Static LAN IP would be antithetical to the device's common usage.

Step 1: Direct Your Browser to the Port Triggering Configuration Page

- 1.A Select the [“Security”](#) tab located within the left-hand frameset.

Then, in the left-hand frameset, select [“Port Triggering”](#)




The screenshot shows the VisionNet web interface. On the left, a navigation tree is visible with the following items: Gateway QuickView, WAN, LAN, Security (expanded), Quality of Service, Routing, DNS, Print Server, Network Access Storage, Service Groups, IPSEC, Certificates, Wireless, Gateway Diagnostics, and Gateway Statistics. Under the 'Security' tab, the following sub-items are listed: Incoming IP Filtering, Outgoing IP Filtering, URL Filtering, Port Forwarding, Port Triggering (highlighted), Multi Nat, DMZ Host, Algorithm, UTM, WAN Access Control, and Bridge Access Control. The main content area is titled 'NAT -- Port Triggering Setup' and contains a table with the following structure:

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

Below the table are 'Add' and 'Remove' buttons. A paragraph of text explains that some applications require specific ports to be opened for access by remote parties, and that Port Trigger dynamically opens up '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.

- 1.B Select the [“Add”](#) Button.

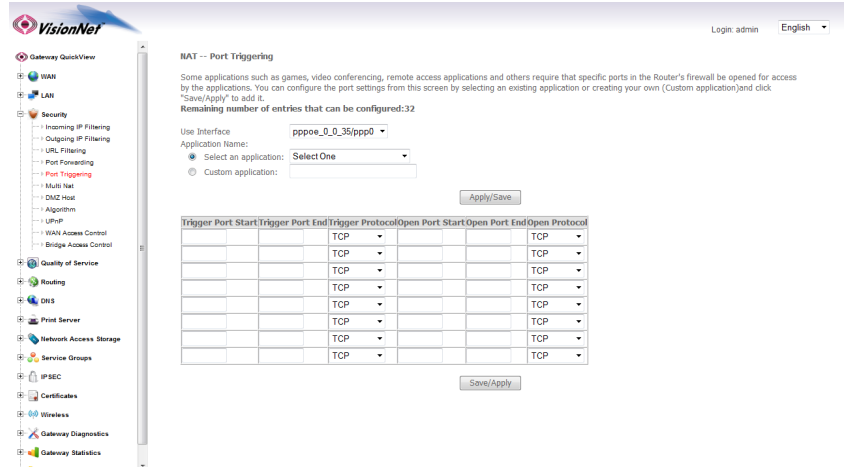
 **Please Note: If the port to be assigned is already specified in the existing Port Triggering Table, you must remove the rule containing this port prior to creating a new one.**

Step 2: Configure the Port Forwarding Rule

2.A Select the appropriate WAN Interface

If the Service you would like to have is already available in the [“Select a Service”](#) menu, you may select this service for auto-population.

You may create a custom Service by selecting [“Custom Application”](#) and entering a new rule name



2.B Enter the port rules

Trigger Port Start This is the port that the LAN device uses to initiate a session

This will usually match the “Trigger Port Start” parameter; some applications, however, may use a succession of ports.

Trigger Port End In this case you will enter the final port in that range.

If these ports are not in succession, must enter the next port as another in the rule

Protocol This should be “TCP/UDP” to avoid possible errors due to end-user communication

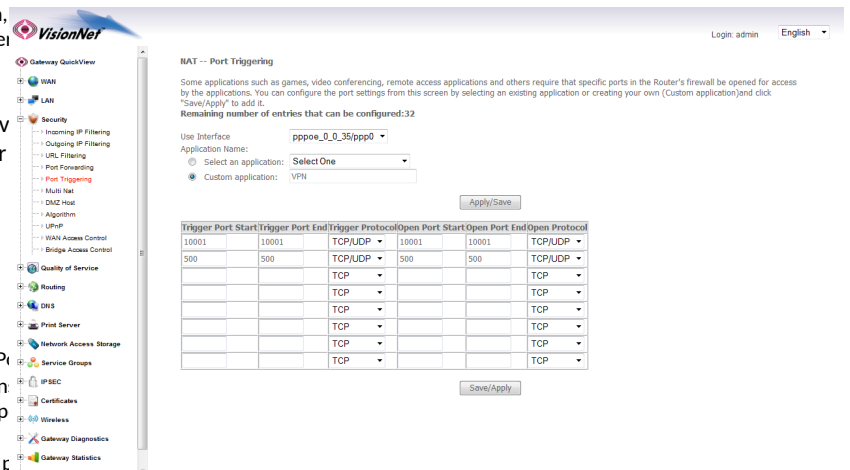
Open Port Start This is the WAN Port that the remote server will reply on

This will usually match the “Open Port Start” parameter; some application however, may use a succession of p

Open Port End In this case you will enter the final port in that range.

If these ports are not in succession, you must enter the next port as another row in the rule

Open Port Protocol This should be “TCP/UDP” to avoid possible errors due to end-user miscommunication



2.C Select “Save/Apply”

2.D Considerations

It may be difficult to determine which ports must be used for a particular application. It is best to specify the LAN device as the DMZ host to see if this resolves the issue.

If this does not resolve the issue, the port triggering rule should be removed and replaced with port forwarding. Once port forwarding has been verified to work then port triggering may be re-visited. If port triggering does not work, then further research should be done to identify the behavior of the communication between the LAN device and the Server.

Section 6.3 – DMZ Host

DEFINITION OF DMZ Host

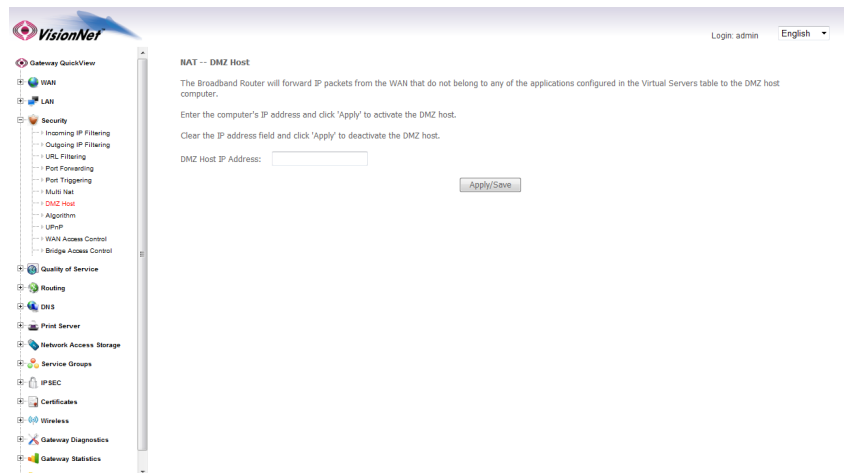
In the event that a remote application attempts to communicate via an inactive, or unspecified, port; the port will be dynamically forwarded to the IP Address specified as the DMZ Host.

If a specific device is to be assigned as a DMZ host, this device should have either a Static IP or a Reserved IP.

Step 1: Direct Your Browser to the DMZ Host Configuration Page

- 1.A Select the **“Security”** tab located within the left-hand frameset.

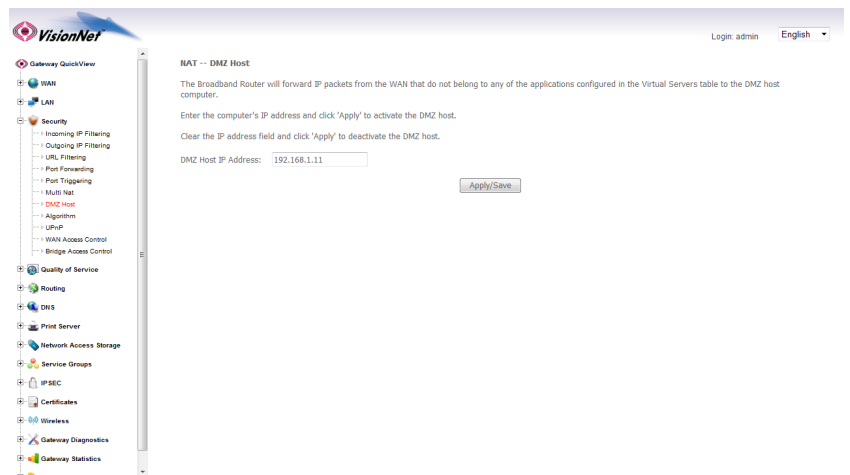
Then, in the left-hand frameset, select **“DMZ Host”**



- 1.B Enter the desired DMZ Host IP Address

This is the IP Address of the LAN Device which will receive all non-specified traffic.

This device should have either a Static IP or Reserved IP



- 1.C Select the **“Save/Apply”** Button.

Section 6.4 - UPnP

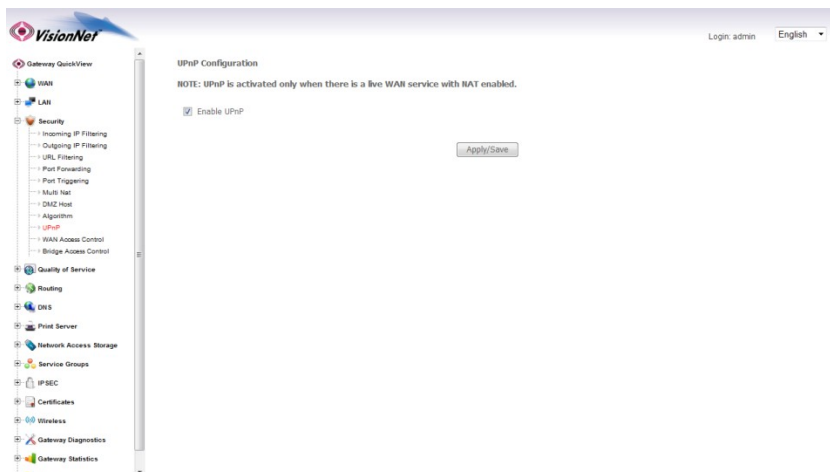
UPnP Definition

Some applications, such as the XBOX, will require UPnP for operation. UPnP will dictate how devices share information on the LAN, and the Dynamic port rules to be used for Internet Content.

Step 1: Direct Your Browser to the UPnP Page

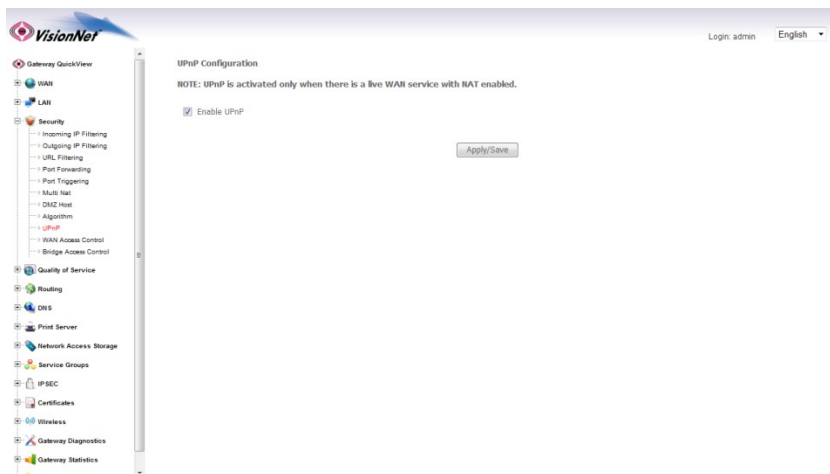
- 1.A Select the [“Security”](#) tab located within the left-hand frameset.

Then, in the left-hand frameset, select [“UPnP”](#)



- 1.B Select [“Enable UPnP”](#)

You may enable / disable UPnP by toggling the checkbox.



- 1.C Select [“Apply Save”](#)

Section 6.5 – Algorithm Enable / Disable

Algorithms Defined

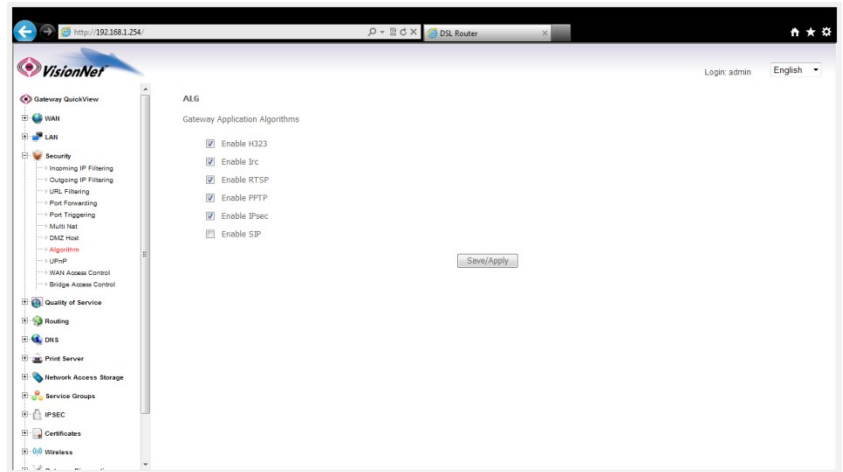
The VisionNet gateway can open ports, based on industry standards and conventions, when certain traffic is detected. You must enable or disable these algorithms to adjust operation.

These algorithm port conventions are only honored when the Firewall is enabled

Step 1: Direct Your Browser to the Algorithm Page

- 1.A Select the **“Security”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“Algorithm”**



- 1.B Enable / Disable Algorithms

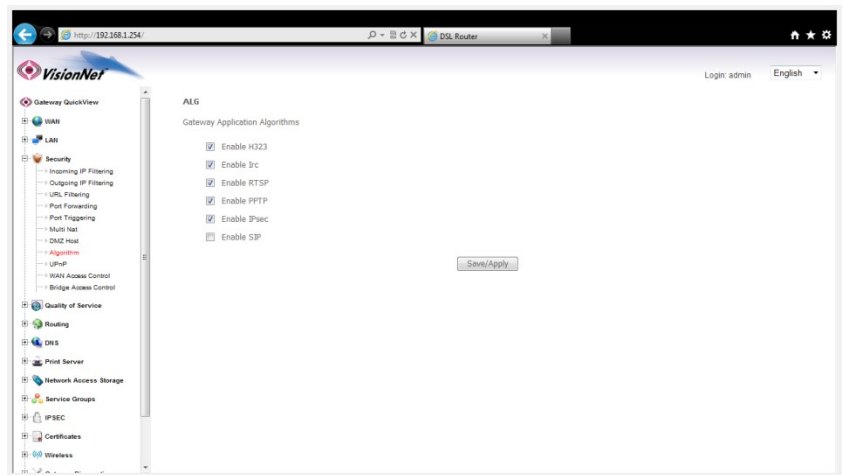
H323

IRC

RTSP

IPSEC

SIP



- 1.C Select **“Apply Save”**

Section 6.6 – WAN Access Control (Parental Controls)

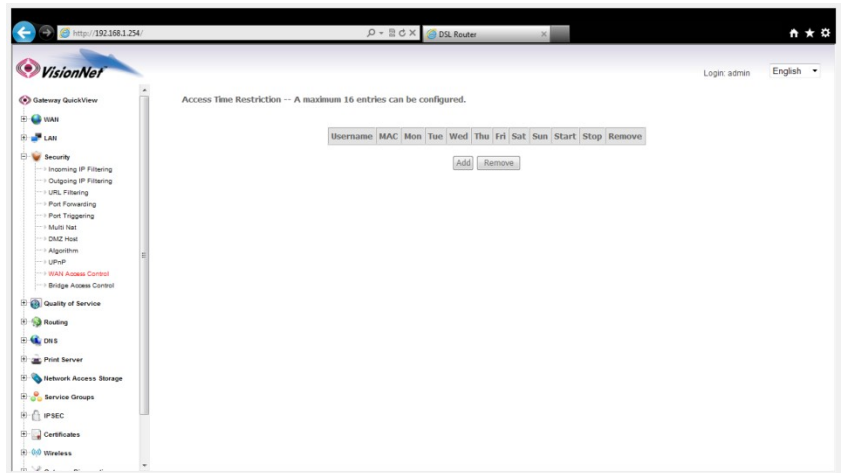
WAN Access Control

The VisionNet Gateway can allow / disallow WAN Access to LAN hosts by a weekly time schedule. MAC Addresses are used to identify devices.

Step 1: Direct Your Browser to the WAN Access Control Page

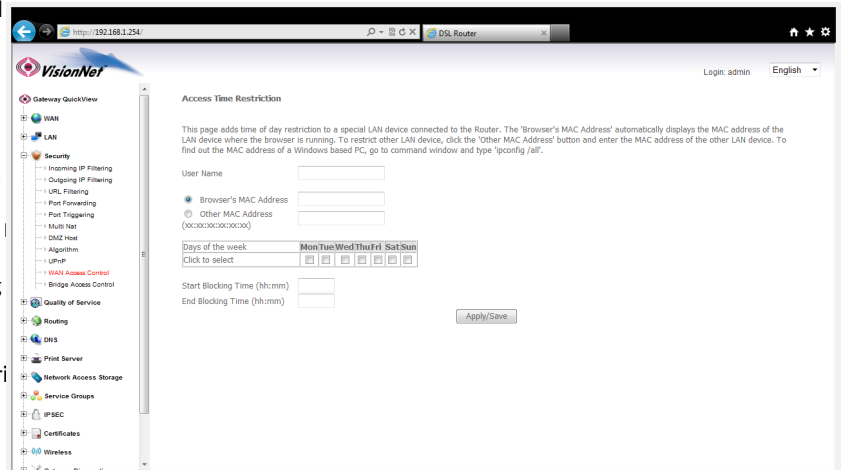
- 1.A Select the **“Security”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“WAN Access Control”**



- 1.B Define Access Time Restrictions

UserName	This is simply for organizational purposes and does not affect performance
MAC Address	Browser's MAC Address: MAC Address of host accessing the Other MAC Address: User Defined Address
Days of the Week	Days of the Week that Blocking be applied
Start / Stop Blocking Time	Time where device will be restricted from the WAN



- 1.C Select **“Apply Save”**

Section 6.7 – URL Filtering (Parental Controls)

URL Filtering

The VisionNet Gateway can allow / disallow access to certain URLs.

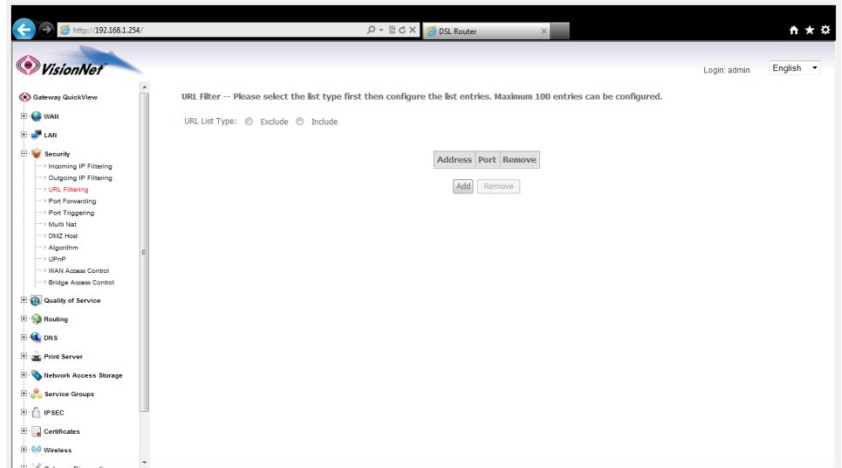
Step 1: Direct Your Browser to the WAN Access Control Page

- 1.A Select the **“Security”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“URL Filtering”**

Include: Only the approved URLs will be allowed

Exclude: Only the disallowed URLs will be blocked



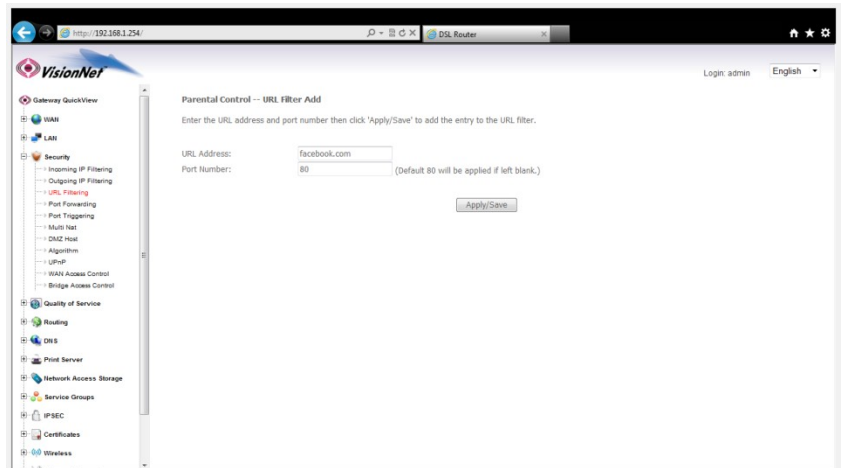
- 1.B Define URL Restrictions

URL

IE: facebook.com

Port Number

80 by default



- 1.C Select **“Apply Save”**

Section 6.8 – IP Filtering

IP Filtering

You may restrict inbound or outbound traffic based upon Layer 3 Identification

Step 1: Direct Your Browser to the WAN Access Control Page

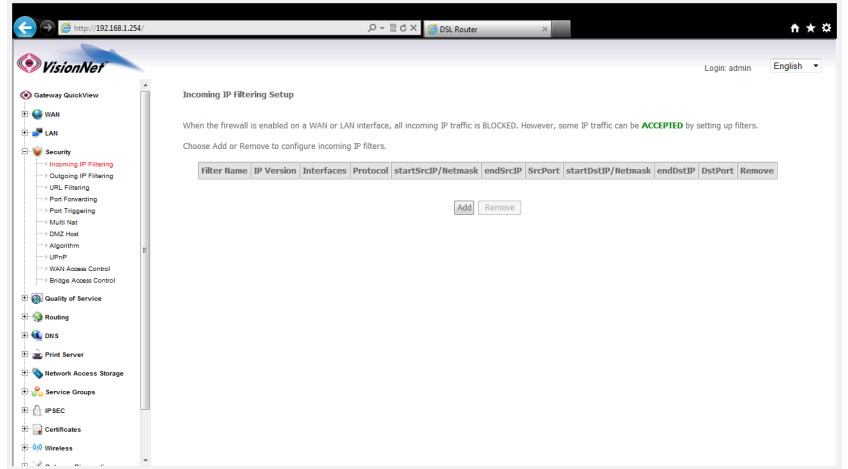
- 1.A Select the **“Security”** tab located within the left-hand frameset.

Then, In the left-hand frameset, select either:

Inbound IP Filtering

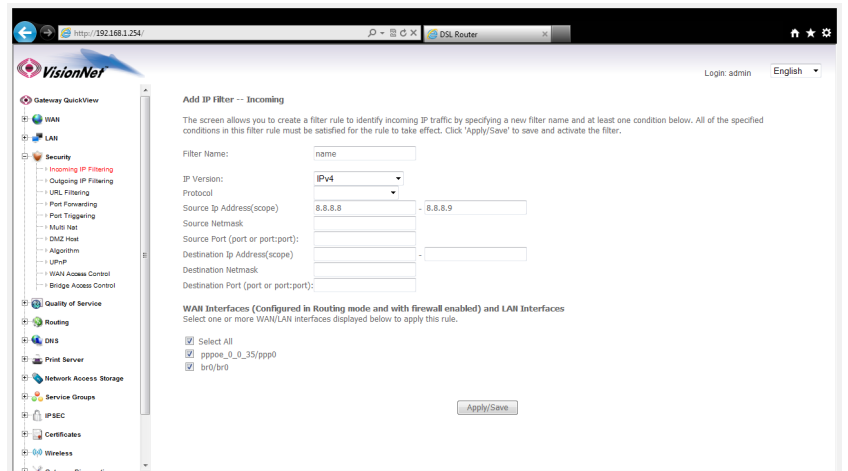
OR

Outbound IP Filtering



- 1.B Define IP Filtering

Define at least one condition for identification of traffic



- 1.C Select **“Apply Save”**

Section 6.9 – Bridge Access Control

Bridge Access Control

You may restrict or allow MAC based traffic for Bridge Interfaces

Step 1: Direct Your Browser to the WAN Access Control Page

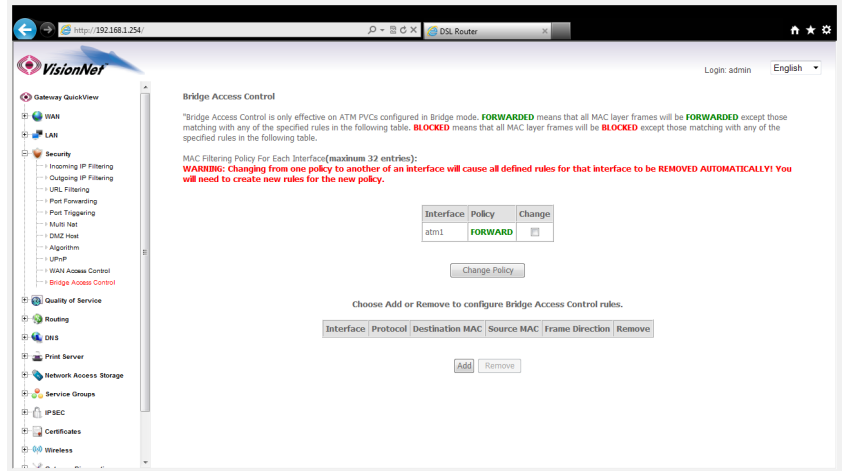
- 1.A Select the **“Security”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select either:

Bridge Access Control

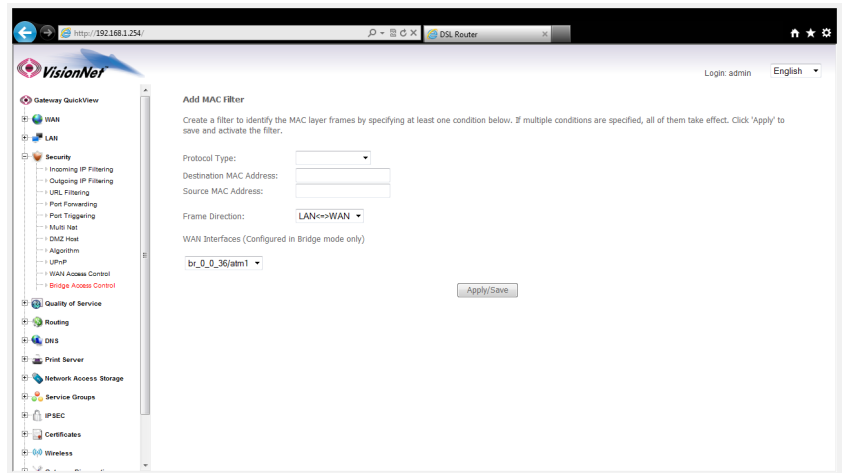
Forwarded: Everything forwarded except defined traffic

Blocking: Everything Blocked except defined traffic



- 1.B Define Restrictions

Define at least one condition for identification of traffic



- 1.C Select **“Apply Save”**

SECTION 7: Quality of Service

Section 7.1: QoS Enable / Disable

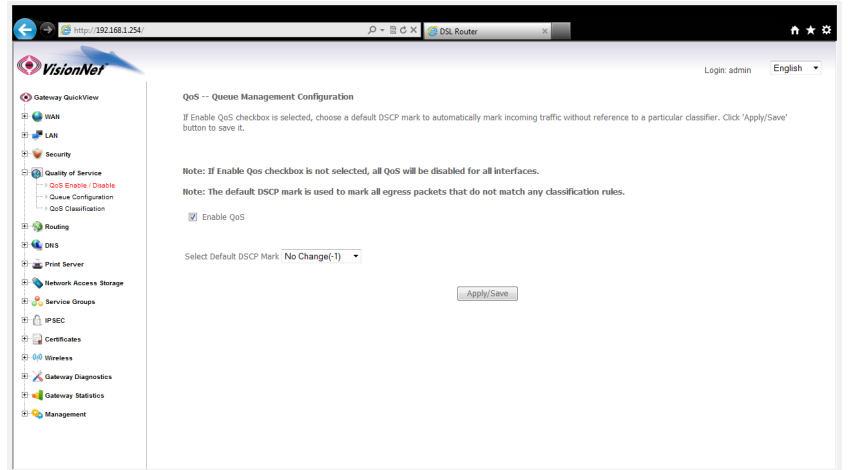
Step 1: Access the QoS Enable / Disable Page

- 1.A Select the **“Quality of Service”** tab located within the left-hand frameset.

You may Enable QoS

Unless specified otherwise, do not change the Default DSCP Mark

This will enable QoS rules within the device



- 1.B Select **“Save / Apply”**

Section 7.2 – QoS Interface Configuration

You may add, enable, and remove the QoS Interface Prioritization Table within this page.

Step 1: Direct Your Browser to the QoS Interface Configuration Page

- 1.A Select the **“Security”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select:

Queue Configuration

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 4 queues can be configured.
If you disable WMM function in Wireless Page, queues related to wireless will not take effect.

The QoS function has been disabled. Queues would not take effect.

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority 1	1	wi0	SP	1				Enabled	
WMM Voice Priority 2	2	wi0	SP	2				Enabled	
WMM Voice Priority 3	3	wi0	SP	3				Enabled	
WMM Video Priority 4	4	wi0	SP	4				Enabled	
WMM Best Effort 5	5	wi0	SP	5				Enabled	
WMM Background 6	6	wi0	SP	6				Enabled	
WMM Background 7	7	wi0	SP	7				Enabled	
WMM Best Effort 8	8	wi0	SP	8				Enabled	
Default Queue 33	33	atm0	SP	8			Path0	<input type="checkbox"/>	<input type="checkbox"/>
Default Queue 34	34	atm1	SP	8			Path0	<input type="checkbox"/>	<input type="checkbox"/>

- 1.B Enable / Disable Rules

You must enable a rule for it to take precedence. You may also create Queue precedence for interfaces within this section

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 4 queues can be configured.
If you disable WMM function in Wireless Page, queues related to wireless will not take effect.

The QoS function has been disabled. Queues would not take effect.

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority 1	1	wi0	SP	1				Enabled	
WMM Voice Priority 2	2	wi0	SP	2				Enabled	
WMM Video Priority 3	3	wi0	SP	3				Enabled	
WMM Video Priority 4	4	wi0	SP	4				Enabled	
WMM Best Effort 5	5	wi0	SP	5				Enabled	
WMM Background 6	6	wi0	SP	6				Enabled	
WMM Background 7	7	wi0	SP	7				Enabled	
WMM Best Effort 8	8	wi0	SP	8				Enabled	
Default Queue 33	33	atm0	SP	8			Path0	<input type="checkbox"/>	<input type="checkbox"/>
Default Queue 34	34	atm1	SP	8			Path0	<input type="checkbox"/>	<input type="checkbox"/>

- 1.C Select **“Apply Save”**

Section 7.3 – QoS Classification

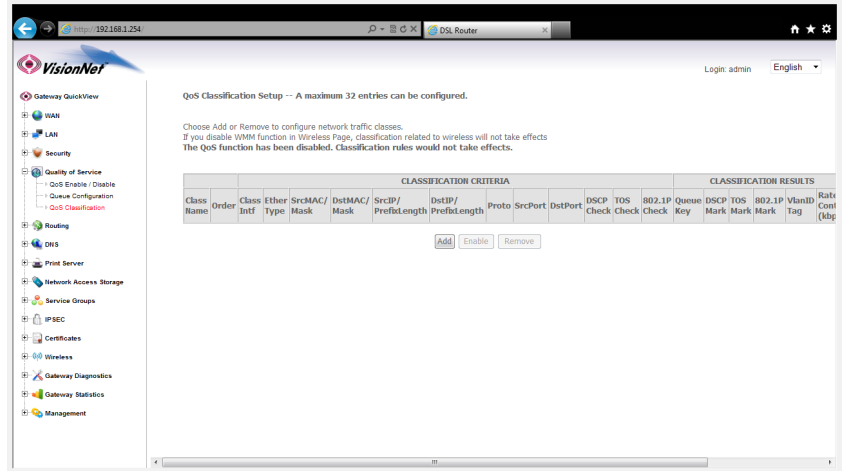
You may add, enable, and remove the QoS Configuration

Step 1: Direct Your Browser to the WAN Access Control Page

- 1.A Select the **“Security”** tab located within the left-hand frameset.

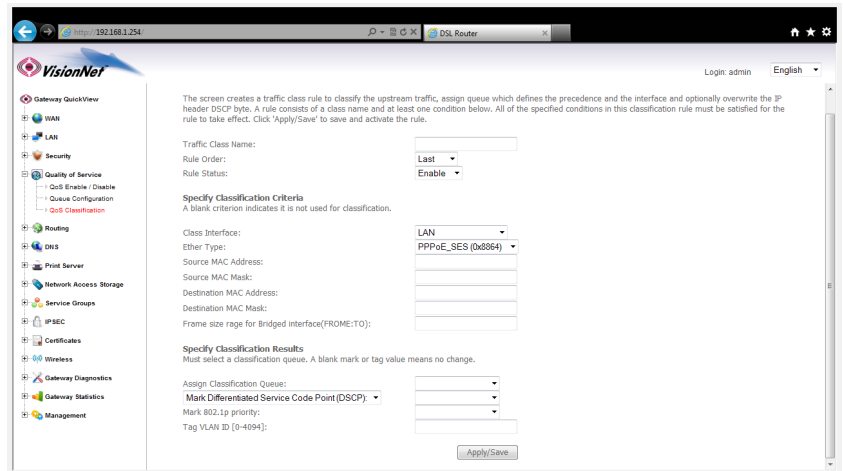
Then, in the left-hand frameset, select:

QoS Classification



- 1.B Create a new QoS Classification

You may identify and modify QoS tagging within this table



- 1.C Select **“Apply Save”**

SECTION 8: Service Grouping

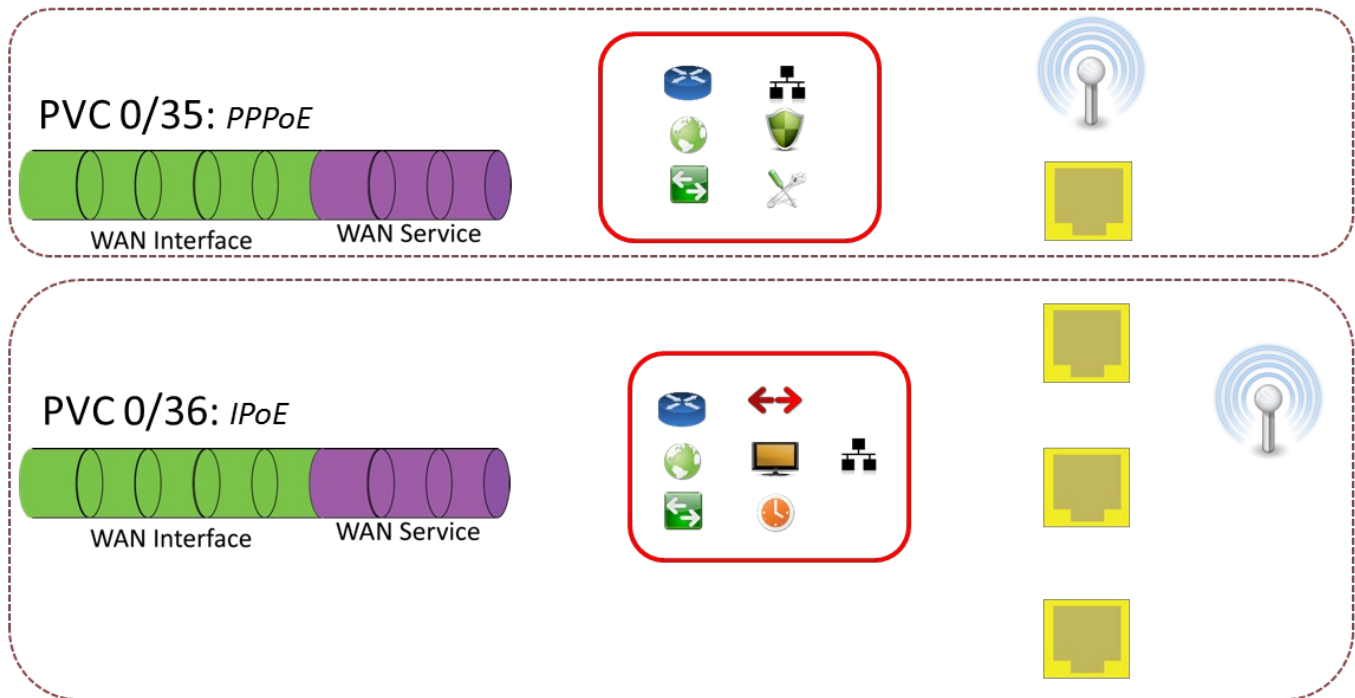
Section 8.1: Service Group Logic

The Service Group Operates similarly to port mapping of the past. A WAN interface may provide service, to particular Interfaces, independent of other services.

The key difference between Service Grouping, and Port Mapping of the past, is that the VisionNet device supports multiple NAT Sessions, DHCP Servers, and Network Conventions between Service Grouping.

A Service Group, Therefore, Operates similarly to a traditional VLAN; except that the VLAN Tagging conventions are transparent to the administrator.

Group's IP Services Operate Independently of Each Other



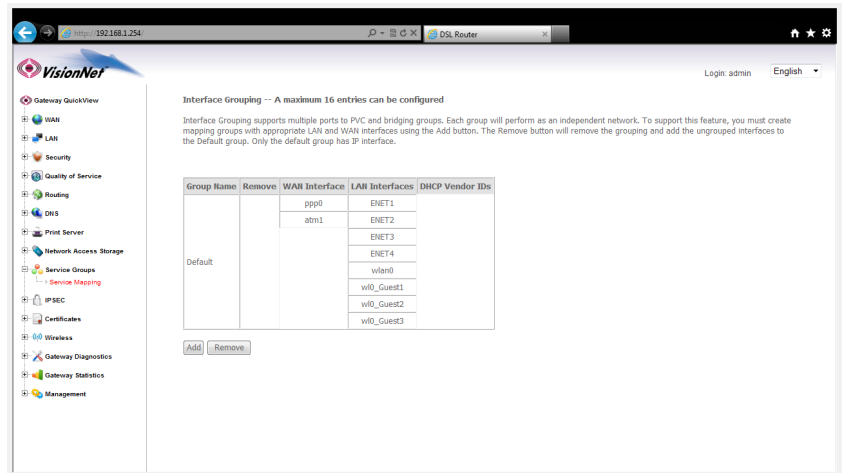
Section 8.2 – Service Group Creation

Step 1: Direct Your Browser to the Service Group Page

- 1.A Select the [“Service Groups”](#) tab located within the left-hand frameset.

Then, in the left-hand frameset, select:

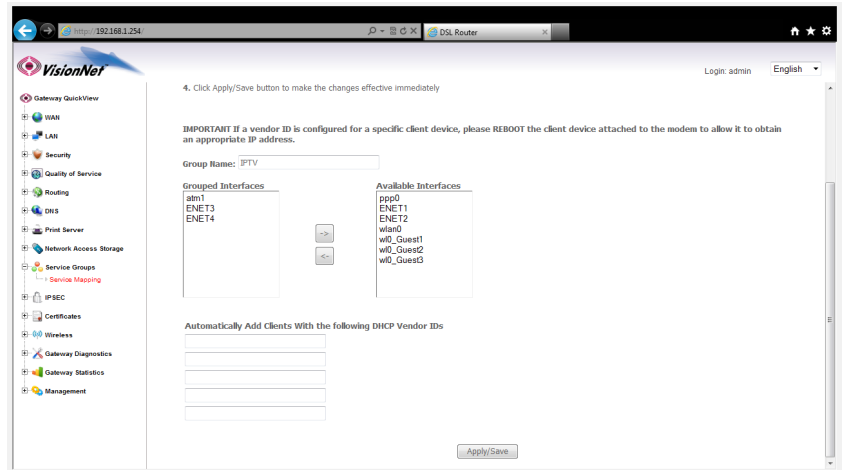
[Service Mapping](#)



- 1.B Select Add

You may select physical interfaces to be grouped together with specific WAN services. These will operate independently of the primary gateway operation.

You may also group clients by DHCP Vendor IDs (Boot P Classification)



- 1.C Select [“Apply Save”](#)

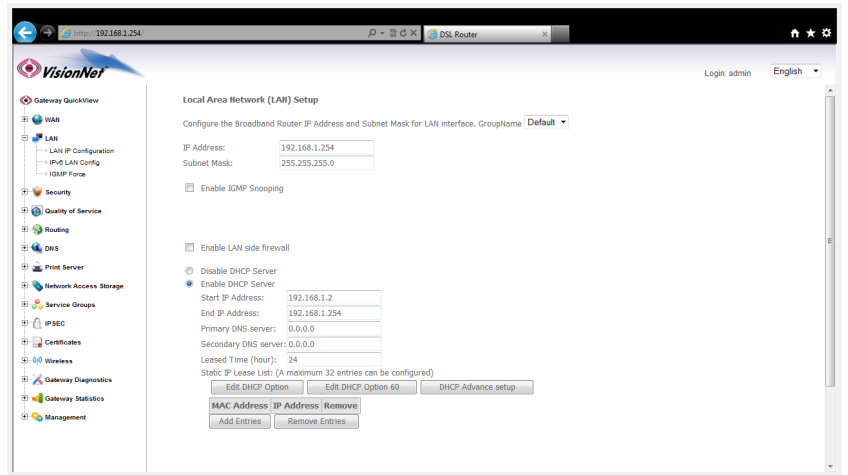
Section 8.3 – Service Group LAN Management

Step 1: Direct Your Browser to the LAN Page

- 1.A Select the **“LAN”** tab located within the left-hand frameset.

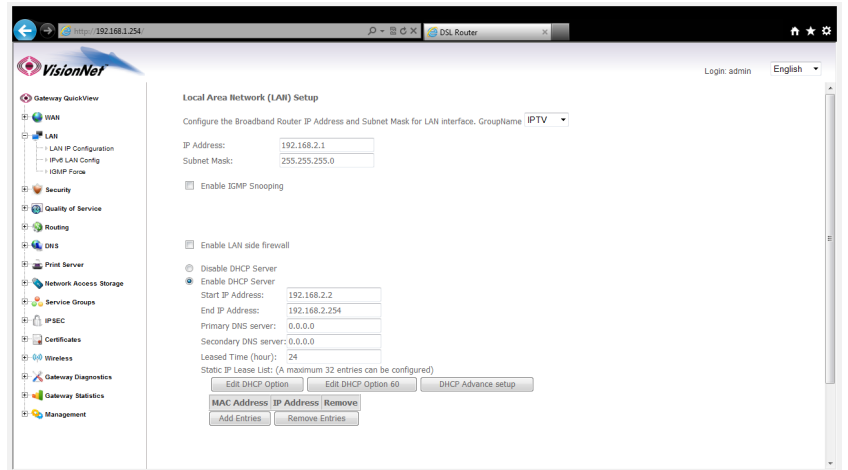
Then, in the left-hand frameset, select:

LAN IP Management



- 1.B Select the appropriate GroupName





You may configure the Service Group LAN Settings independent of the Primary Service Group



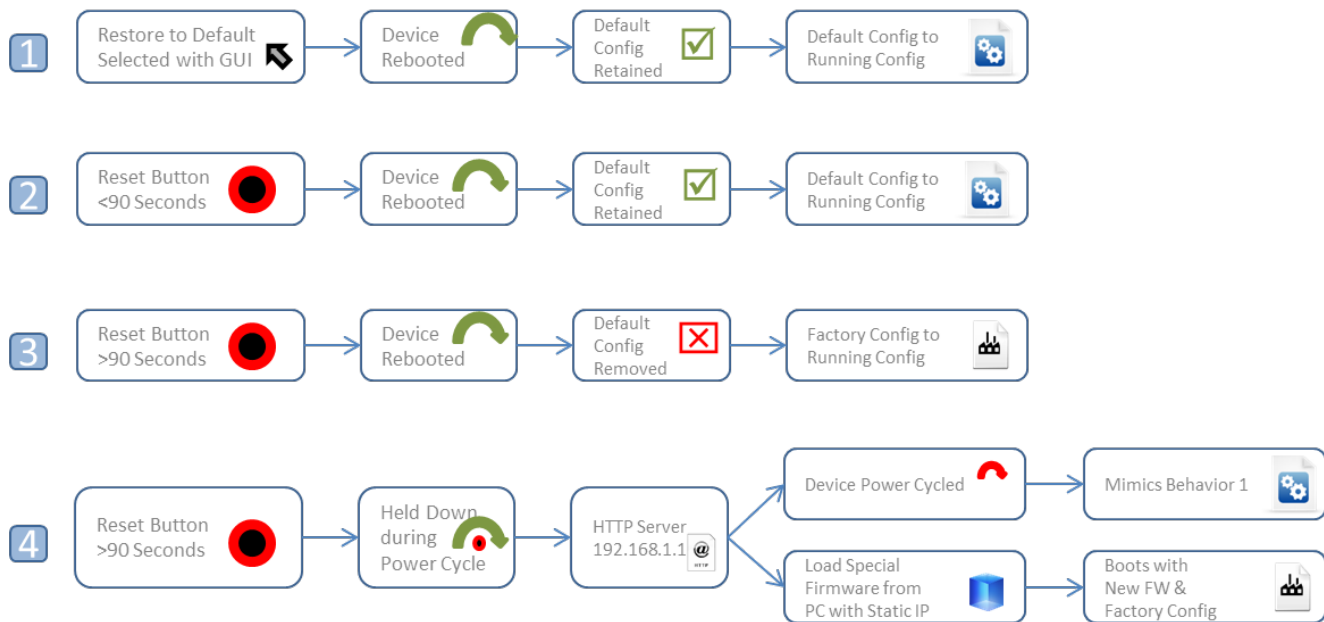
- 1.C Select **“Apply Save”**

SECTION 9: CONFIGURATION SETTINGS

Section 9.0 - Configuration File Logic

	Running Configuration	◆ Configuration in Use
	Startup Configuration	◆ Automatically updated from Running Configuration
	Default Configuration	◆ Default Settings retained during "reset"
	Factory Configuration	◆ Only accessible from a board reclaim

Device Reset Behavior



Section 9.1 – Save Backup Configuration

When to save the Backup Configuration:

Prior to making remote changes to the modem

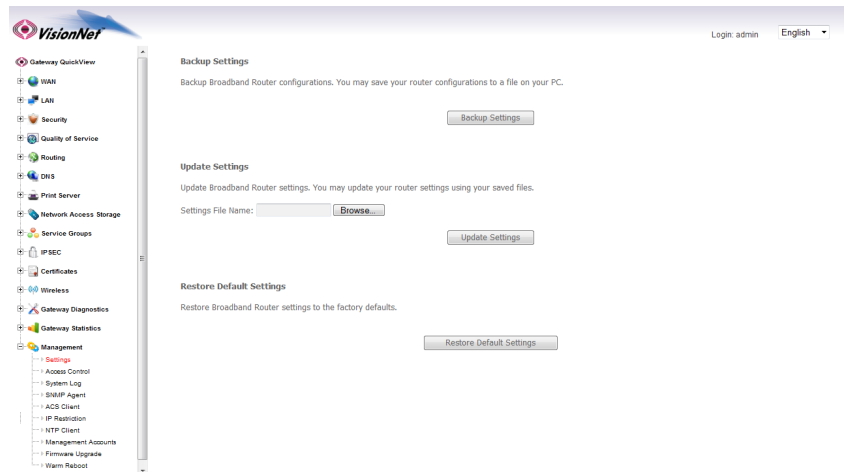
Where to save the backup configuration:

It is suggested that the backup configuration is kept on your PC Desktop and given a customer name

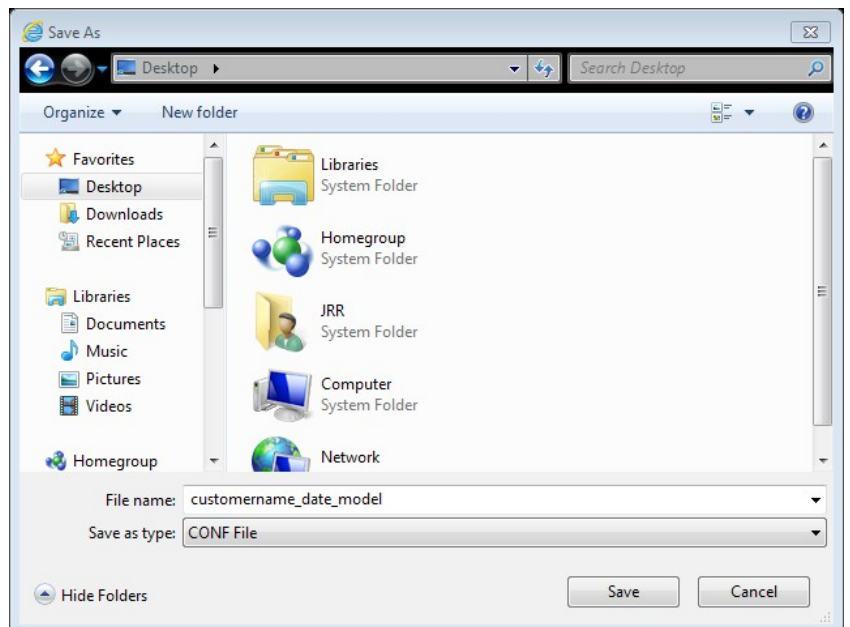
Step 1: Access the GUI to find Backup Configuration Tool

- 1.A Select the **“Management”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“Settings”**



- 1.B Select **“Backup Settings”** and choose your download location via your browser’s download tool.



Section 9.2 – OverWrite Default Configuration

When to update the default configuration:

ONLY UPDATE THE DEFAULT CONFIGURATION WITH APPROVAL FROM A SUPPORT MANAGER.

The VisionNet modem comes with a pre-configured default configuration. In the event that you would like to access the original configuration, please ask the customer to hold the reset button for 5 seconds.

Behavior of the Default Configuration:

The default configuration is loaded to the running configuration when the customer holds the modem's reset button for 5 seconds. It is also loaded to the running configuration when [“Restore Default”](#) is selected within the GUI.

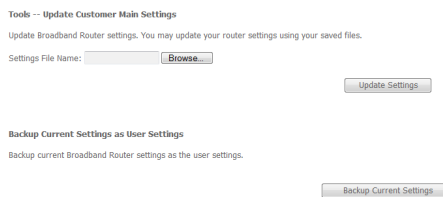
Step 1: Access the GUI to find the Default Configuration Page

1.A The “Update Default Configuration” page is hidden within the GUI to prevent un-authorized access.

The hidden URL is located at :

<http://XXX.XXX.XXX.XXX/customer/main.html>

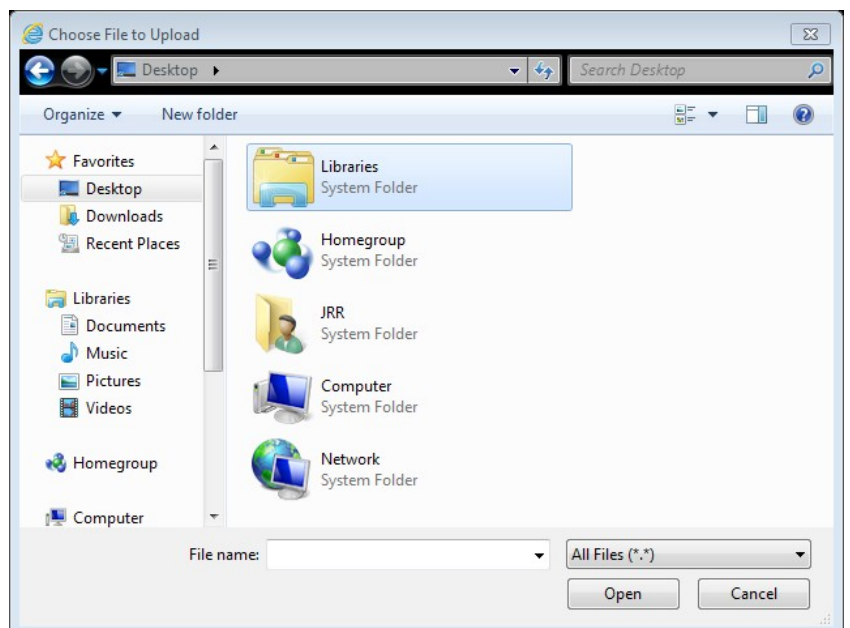
Where **XXX.XXX.XXX.XXX**
Is the IP address of the modem
(either local or remote)



1.B.1 You may select [“Backup Current Settings”](#) to save the running configuration as the default configuration - **OR** -

1.B Select [“Browse”](#) button and choose your file location via your browser's upload tool.

Select the [“Update User Settings”](#) button



Section 9.3 – Update the Running Configuration

When to update the Running Configuration:

When you wish to test new settings without affecting the default configuration.

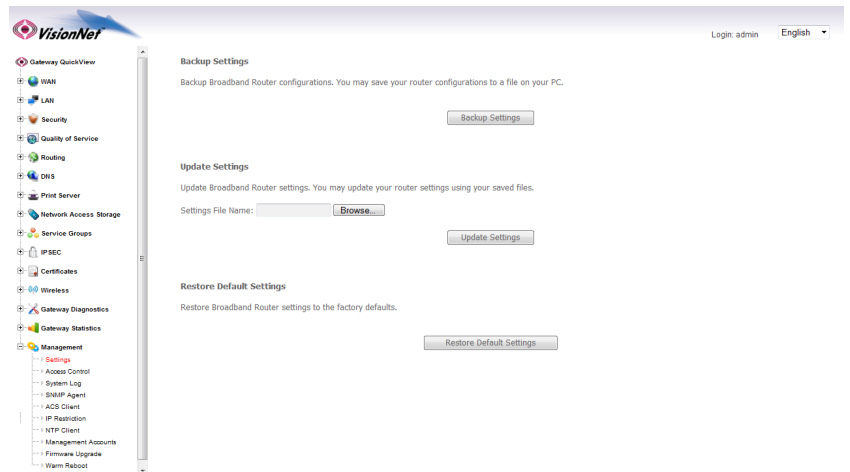
Behavior of the Running Configuration:

The running configuration only affects the modems functionality during operation and standard reboots. It is erased when the customer presses the reset button or the [“Restore Default”](#) function is activated.

Step 1: Access the GUI to find Backup Configuration Tool

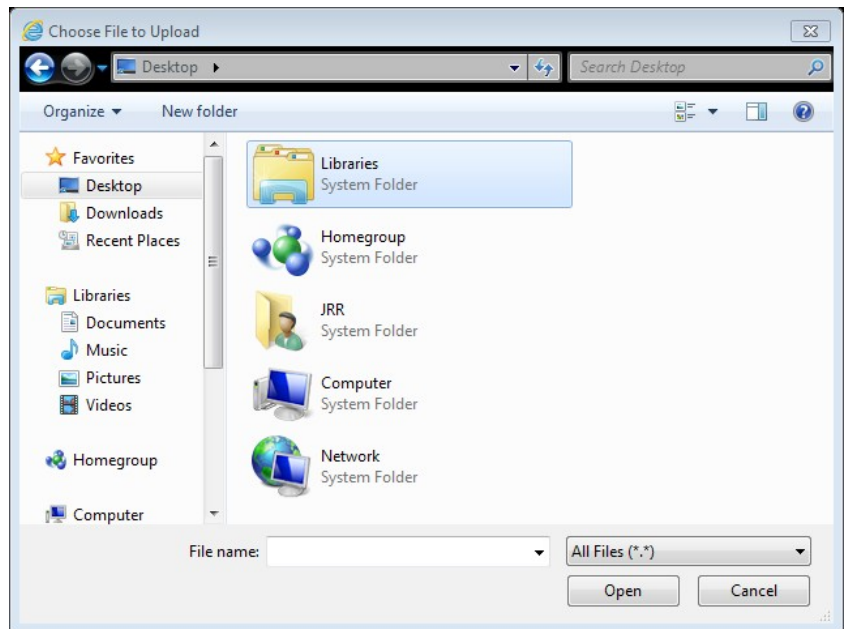
- 1.A Select the [“Management”](#) tab located within the left-hand frameset.

Then, in the left-hand frameset, select [“Settings”](#)



- 1.B Select [“Browse”](#) button and choose your file location via your browser’s upload tool.

Select the [“Update Settings”](#) button



Section 9.4 – Restore the Default Settings

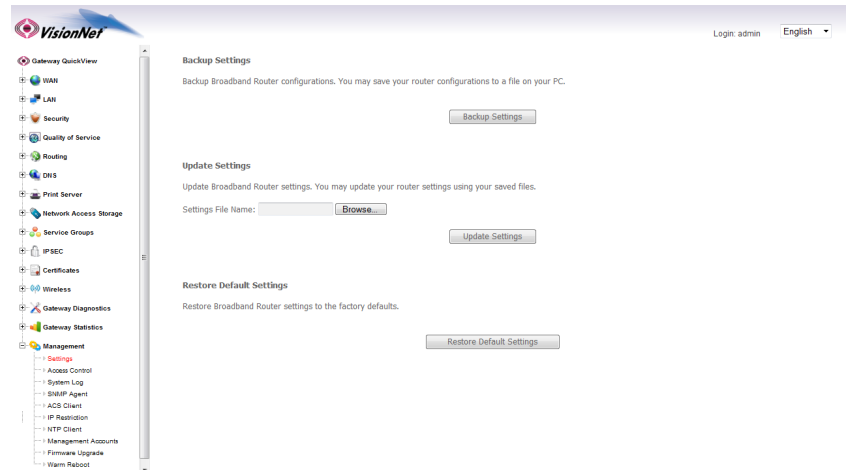
When to Restore the Default Settings

When undocumented changes have been made that limit Internet Access, or the customer has made changes that affect performance.

Restoring the Default Settings via the GUI

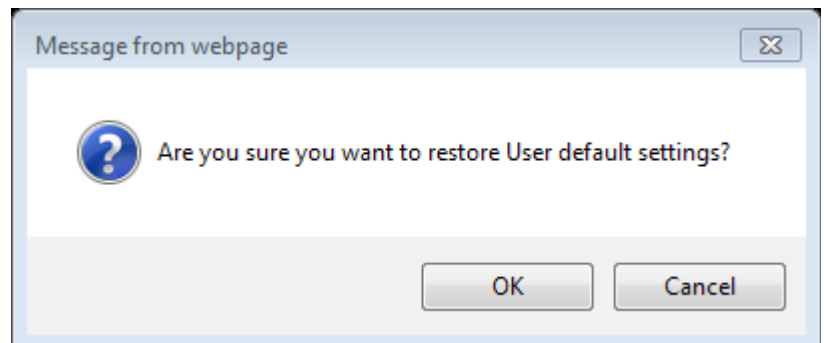
- 1.A Select the **“Management”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“Settings”**



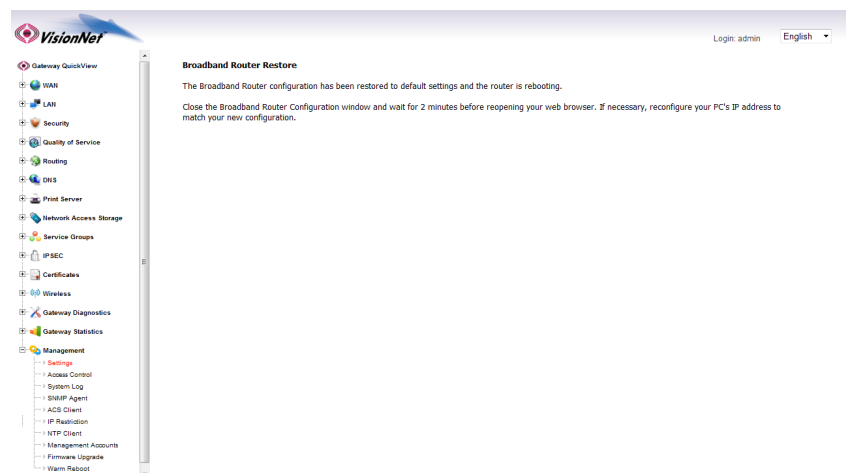
- 1.B Select the **“Restore Default Settings”**.

When challenged, approve the restore.



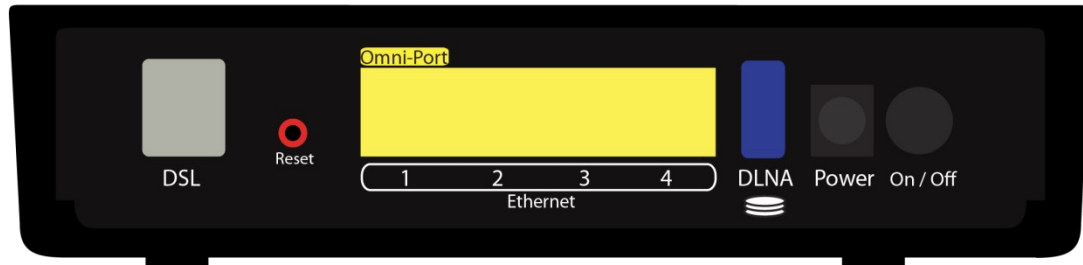
The modem will reset itself. You may need to refresh your browser.

It is possible that the modem will obtain a new IP Address upon reboot.



Restoring the Default Settings via the Reset Button

2.A Press the Reset Button and hold down for 5 seconds



2.B Wait for the modem to reboot

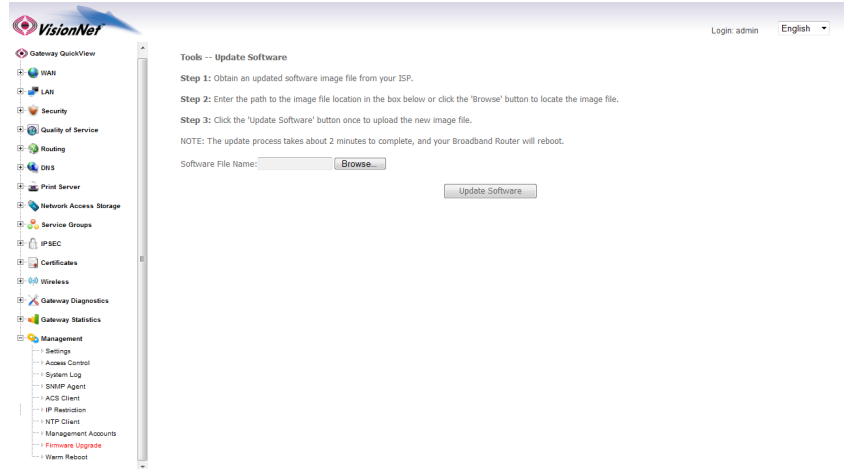
Section 9.5 – Update Firmware

There may be times that you are requested, by a support manager, to update the product software.

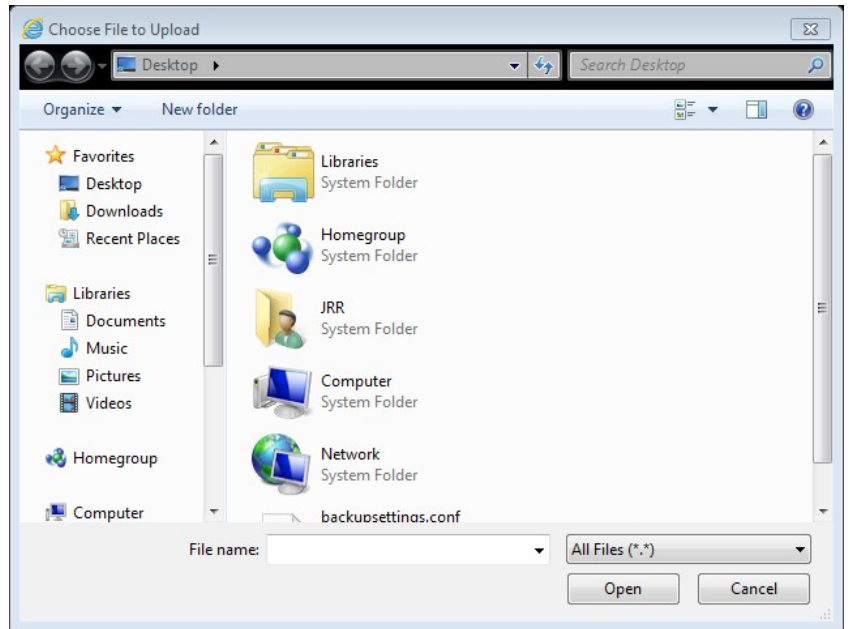
Step 1: Access the GUI to find the Update Firmware Tool

- 1.A Select the **“Management”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“Firmware Upgrade”**



- 1.B Select the **“Browse”** button and select the firmware file on your PC



- 1.C Once you have specified the firmware, select the **“Update Software”** button. The modem will reset itself.

Section 9.6 – Rebooting the Modem

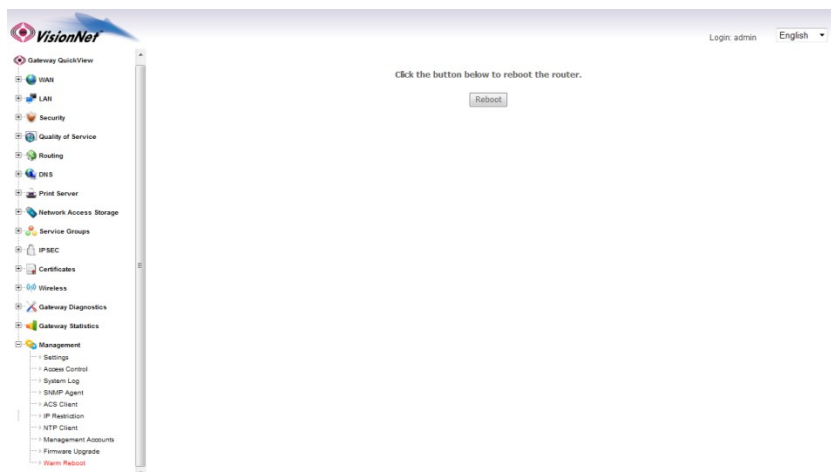
Sometimes, the modem may need to be reset in order for changes to take effect, or to re-initialize network settings.

Rebooting the modem will reboot the modem to the running configuration, not the default configuration.

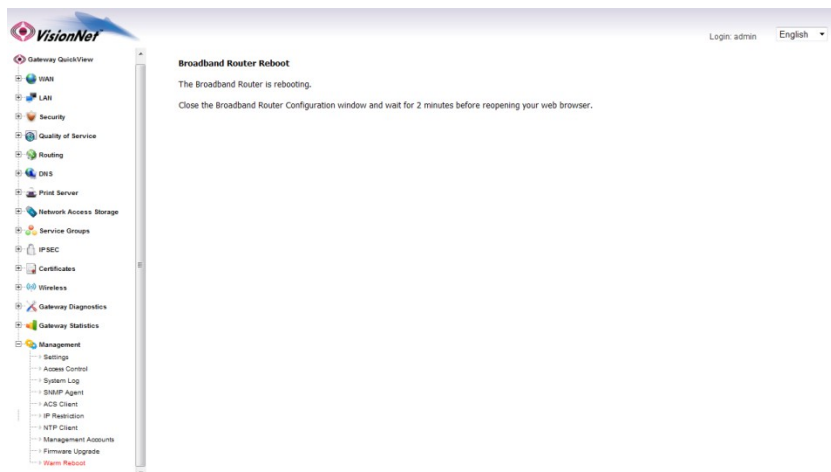
Step 1: Access the GUI to find the Reboot Tool

- 1.A Select the **“Management”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“Warm Reboot”**



- 1.B Select the **“Reboot”** button. The modem will reset itself with the running configuration



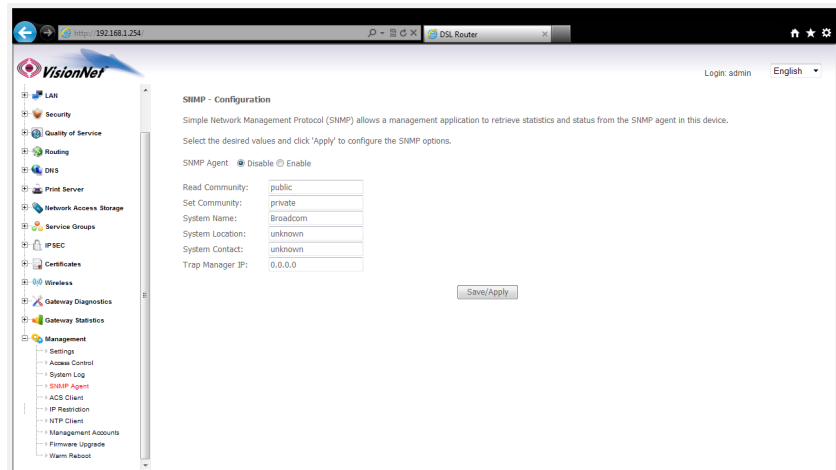
Section 9.7 – SNMP Configuration

SNMP Traps will allow for you to monitor modem performance

Step 1: Access the GUI and find the SNMP Configuration Page

- 1.A Select the **“Management”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“SNMP”**



- 1.B Enter the appropriate information, and the select **“Save/Apply”**

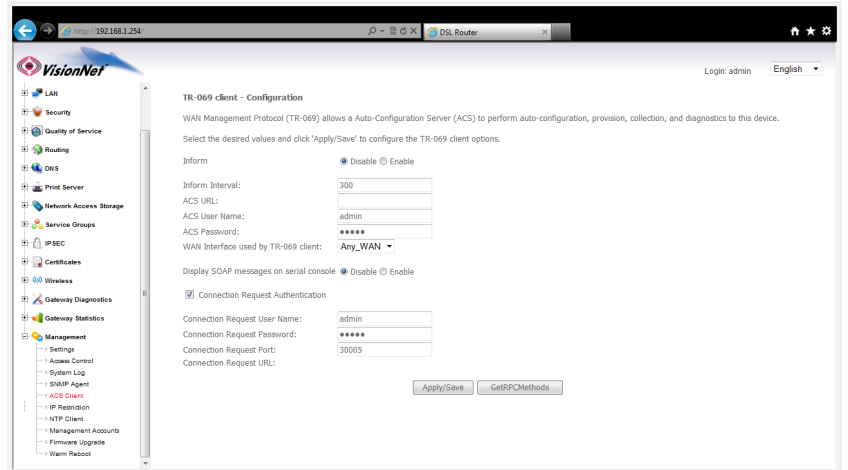
Section 9.8 – ACS Configuration

ACS / TR-069 Servers may be used to access the Gateway.

Step 1: Access the GUI and find the ACS Configuration Page

- 1.A Select the **“Management”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“ACS Client”**



- 1.B Enter the appropriate information, and the select **“Save/Apply”**

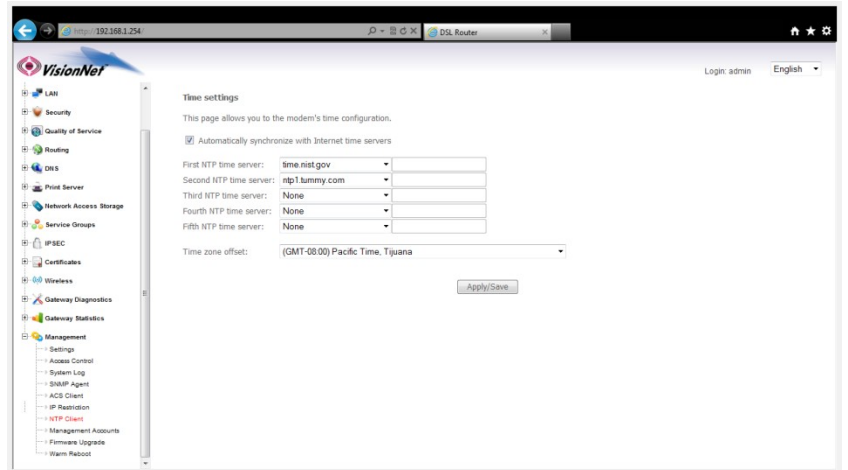
Section 9.9 – NTP Configuration

Network Time Protocol is necessary for accurate SysLog TimeStamps

Step 1: Access the GUI and find the SNMP Configuration Page

- 1.A Select the **“Management”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“NTP”**



- 1.B Enter the appropriate information, and the select **“Save/Apply”**

Section 9.10 – IP Restriction

This will create Access Control Lists for remote and local Access

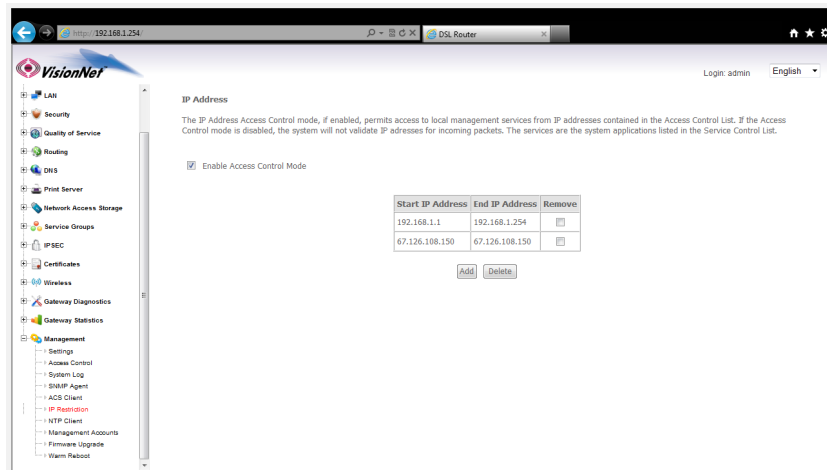
Step 1: Access the GUI and find the SNMP Configuration Page

- 1.A Select the **“Management”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“IP Restriction”**

NOTE: YOU MUST ENTER THE LAN IPs, AND THE APPROPRIATE WAN IPs BEFORE YOU ENABLE THE ACL.

IF YOU ENABLE THE ACL WITHOUT THIS TABLE BUILT, YOU WILL NEED TO DEFAULT THE UNIT



- 1.B Enter the appropriate information, and then select **“Save/Apply”**

Section 9.11 – Remote Access

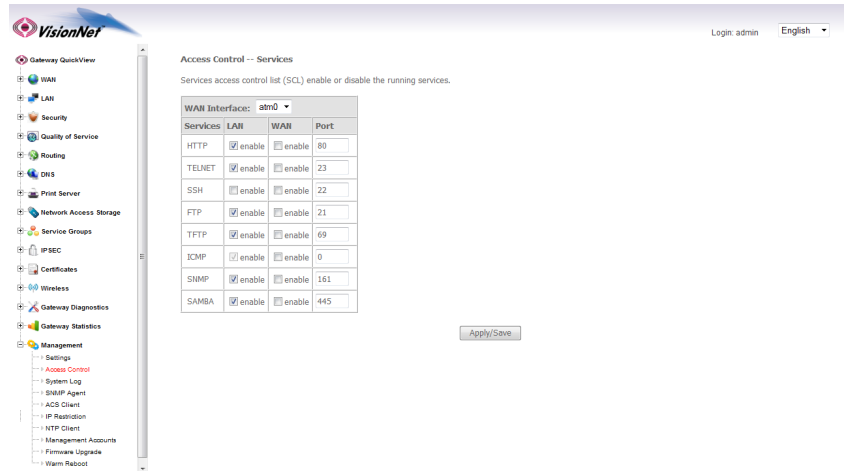
The VisionNet modems come pre-configured to allow remote management access.

Step 1: Access the GUI to find the Remote Access Tool

- 1.A Select the **“Management”** tab located within the left-hand frameset.

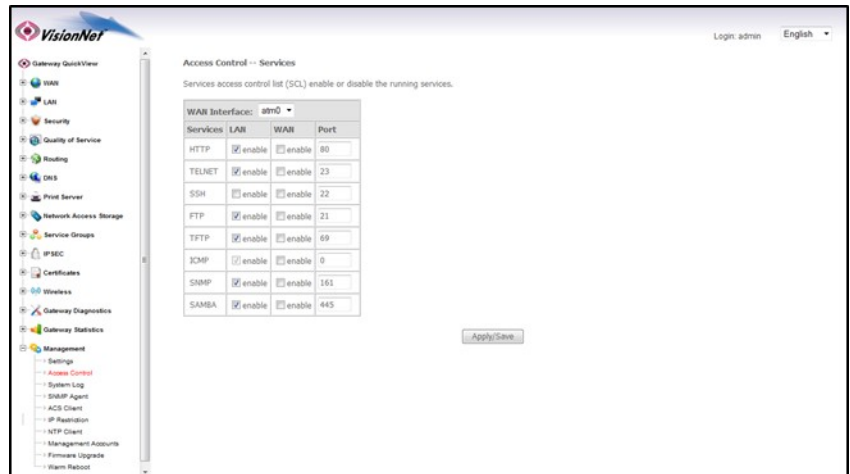
Then, in the left-hand frameset, select **“Access Control”**

Then, in the drop-down box, select **“WAN Interface: ATM 0 or ATM 1”** (Depending upon which network the device is operating)



- 1.B Select / Unselect each option. The Default Settings are specified below

Protocol	LAN	WAN	Port
FTP	<input type="checkbox"/>	<input type="checkbox"/>	21
HTTP	<input type="checkbox"/>	<input type="checkbox"/>	80
ICMP	<input type="checkbox"/>	<input type="checkbox"/>	N/A
SNMP	<input type="checkbox"/>	<input type="checkbox"/>	161
SSH	<input type="checkbox"/>	<input type="checkbox"/>	22
Telnet	<input type="checkbox"/>	<input type="checkbox"/>	23
TFTP	<input type="checkbox"/>	<input type="checkbox"/>	69



- 1.C Select the **“Save / Apply”** button

SECTION 10: WiFi Configuration

Section 10.1 – WIRELESS CHANNEL CONFIGURATION

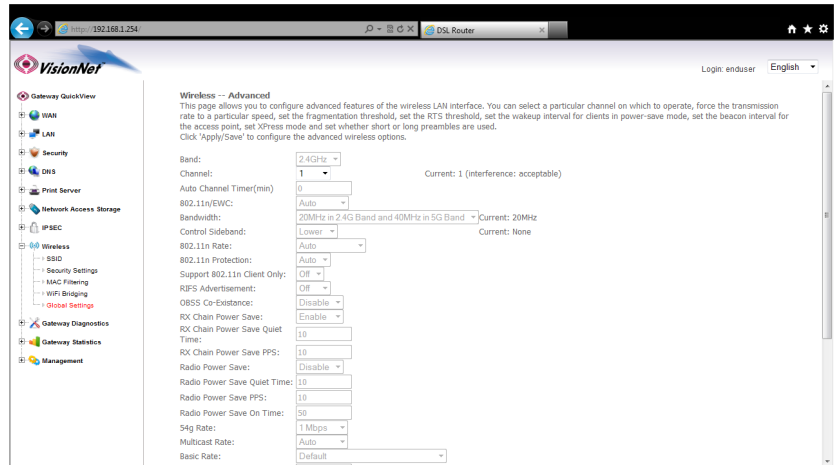
When to change the Wireless Channel.

Many items in your home, and your immediate neighbors' homes, likely use the 2.4 Ghz range. There are 11 possible channels that may be used within this spectrum. If your wireless connection becomes very slow, or drops, there may be other devices that are impeding upon your network. This is when you should consider changing your wireless channel.

Step 1: Direct Your Browser to the Global Wireless Configuration Page

1.A Select the **“Wireless”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“Global Settings”**

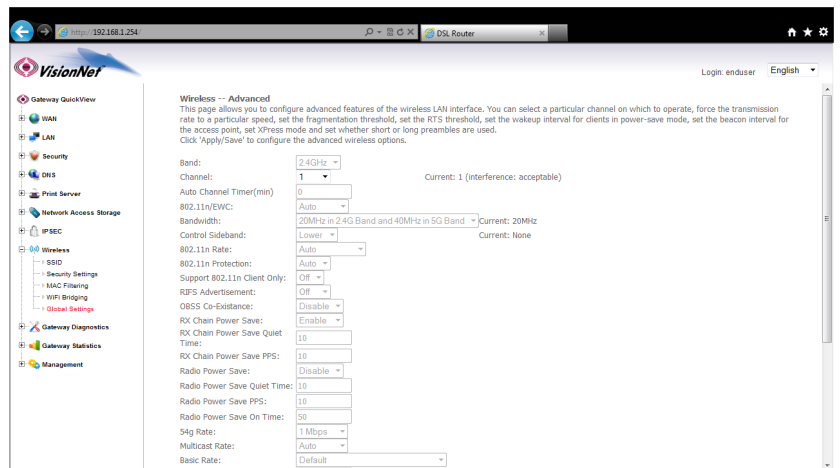


1.B Enter the desired Channel.

1, 6, and 11 tend to operate the best.

Other Channels to consider are 3 and 9.

Once you have selected the new channel, select **“Save/Apply”** at the bottom of the screen.



1.C Select the **“Save/Apply”** Button.

Section 10.2 – SSID CONFIGURATION

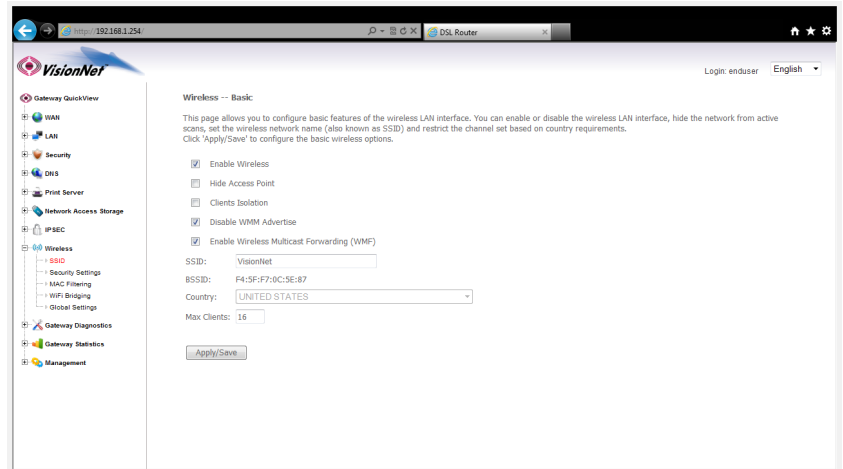
When to change the Wireless SSID

You may wish to broadcast a different network name than the one provided; change the broadcasting conventions; or alter the services advertised by the BSSID.

Step 1: Direct Your Browser to the SSID Configuration Page

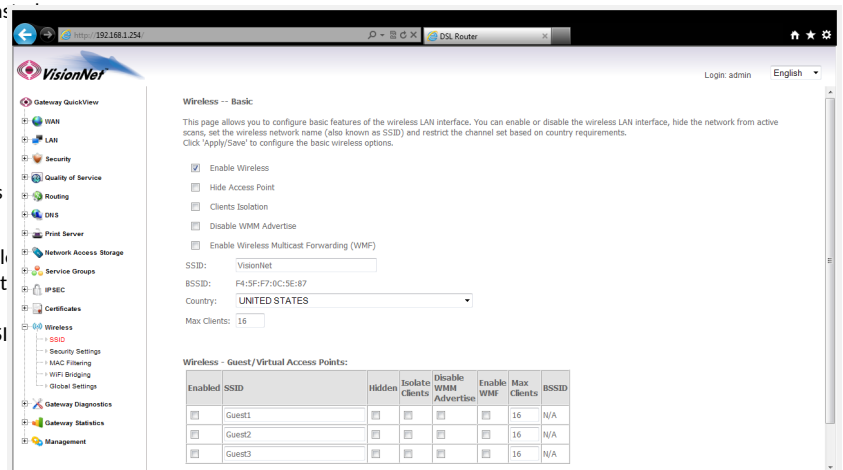
- 1.A Select the **“Wireless”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“SSID”**



- 1.B Enter the new SSID Name

Enable Wireless	Wireless should be enabled
Hide Access Point	The SSID Name will not be broadcast
Clients Isolation	No direct WiFi to WiFi connections
Disable WMM Advertise	This should be enabled.
Enable WMF	This should be enabled; some wireless devices will make Multicast request
SSID	THIS IS WHERE YOU DEFINE THE SSID NAME
BSSID	No modification – this is the MAC Address that is advertised
Country	United States is the support module
Max Clients	Limits the amount of devices that can connect



- 1.C Guest / Virtual SSIDs

- 1.C Select the **“Save/Apply”** Button.

Section 10.3 – WIRELESS ENCRYPTION

When to change the Wireless Encryption

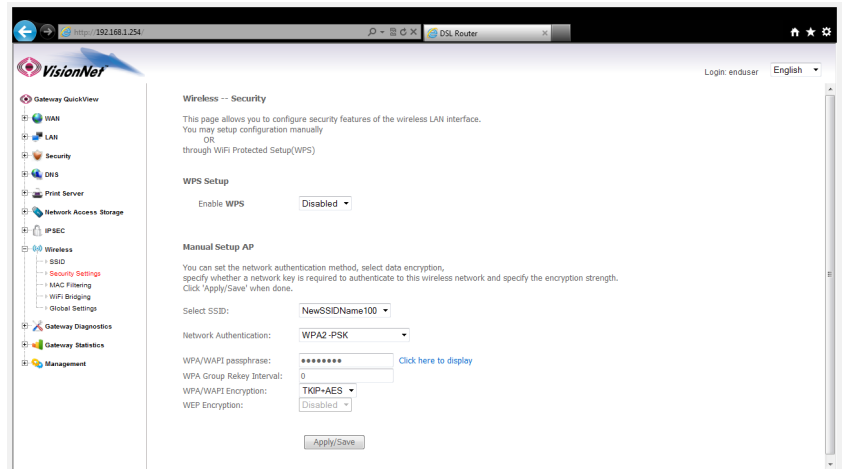
You may wish to use a special login password for your wireless network.

NEVER LEAVE YOUR NETWORK UNENCRYPTED!!! THIS IS VERY INSECURE AND COULD RESULT IN LEGAL TROUBLE SHOULD AN UNAUTHORIZED USER USES YOUR NETWORK FOR ILLEGAL ACTIVITY!

Step 1: Direct Your Browser to the Security Settings Page

- 1.A Select the **“Wireless”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“Security Settings”**



- 1.B Under **“Manual Setup AP”**

Select SSID Choose your network name

Network Authentication

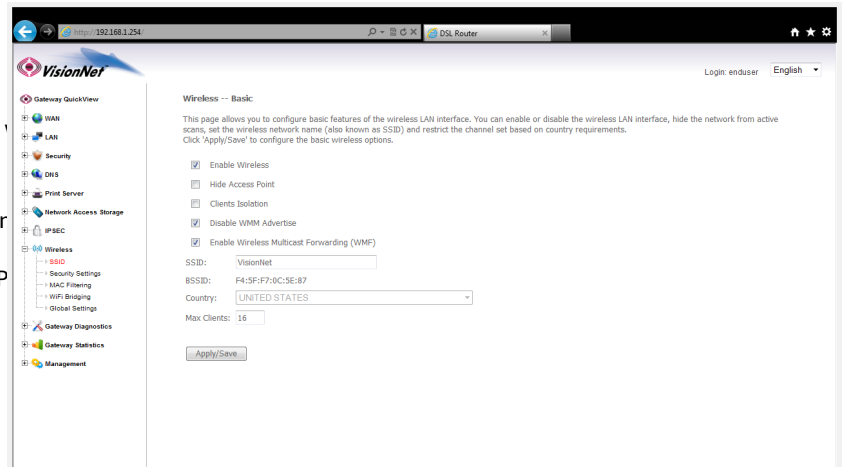
WPA2-PSK is preferable.
Some devices may require PSK
WEP should not be used on the consumer device in question only support WEP

WPA Passphrase Enter the new password

Group Rekey interval 0

AES is preferable

WPA Encryption Some devices may require TKIP+AES



- 1.C Select the **“Click Here to Display”** Button; and verify your encryption key.

- 1.D Select the **“Save/Apply”** Button.

Section 10.4- GLOBAL SETTINGS

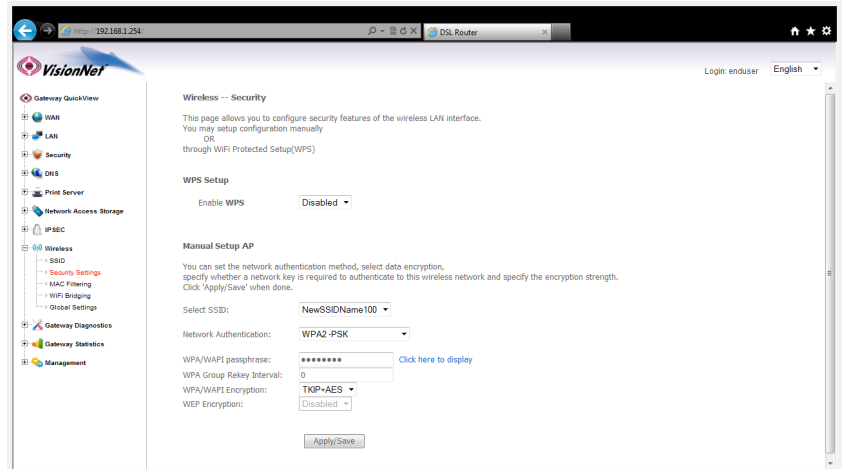
When to change the GLOBAL SETTINGS

Some devices offer very specific support for Wireless. Listed below are the items that may be changed; along with VisionNet suggested settings

Step 1: Direct Your Browser to the Global Settings Page

- 1.A Select the **“Wireless”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“Global Settings”**



- 1.B Under **“Wireless - Advanced”**

BAND	2.4Ghz is the only band supported
Channel	This is selected based upon the network environment
Auto Channel Timer	<p>If the wireless channel is set to Auto, you must specify the timeout-</p> <p>Band: 2.4GHz Channel: 1 Auto Channel Timer(min): 0 802.11n/EWC: Auto Bandwidth: 20MHz in 2.4G Band and 40MHz in 5G Band Control Sideband: Lower 802.11n Rate: Auto 802.11n Protection: Auto Support 802.11n Client Only: Off RIFS Advertisement: Off OBSS Co-Existence: Disable RX Chain Power Save: Enable RX Chain Power Save Quiet Time: 10 RX Chain Power Save PPS: 10</p> <p>Current: 1 (interference: acceptable) Current: 20MHz Current: None</p>
Bandwidth	<p>All devices support 20Mhz</p> <p>Only some devices support Mhz</p> <p>20 Mhz is therefore preferred</p>
Control Sideband	40Mhz operation uses two channels - the second channel is related to the primary channel

- 1.C Under **“Wireless - Advanced”**

802.11N Only	Off	
RIFS Advertisement	Off	
	This is a legacy protocol	
	Off	
OBSS Coexistence	This is used in environments where multiple APs use the same BSSID Name - but this opens up the possibility of hacking if not in a controlled environment	Support 802.11n Client Only: Off
		RIFS Advertisement: Off
		OBSS Co-Existence: Disable
		RX Chain Power Save: Enable
RX Chain Power Save	Off	RX Chain Power Save Quiet Time: 10
	WMM is preferable	RX Chain Power Save PPS: 10
		Radio Power Save: Disable
		Radio Power Save Quiet Time: 10
MultiCast Rate	Auto	Radio Power Save PPS: 10
		Radio Power Save On Time: 50
Basic Rate	Default	54g Rate: 1 Mbps
		Multicast Rate: Auto
		Basic Rate: Default
Xpress Technology	Disabled	Fragmentation Threshold: 2346
	This is only for Broadcom wireless clients - We do not suggest Proprietary Settings used ever	RTS Threshold: 2347
	100%	DTIM Interval: 1
		Beacon Interval: 100
		Global Max Clients: 16
Transmit Power	You may wish to diminish output in MTUs where there are many APs in the area - You cannot, however, control other Consumer Electronics	XPress Technology: Disabled
		Transmit Power: 100%
		WMM(Wi-Fi Multimedia): Enabled
WMM	Enabled - This is required for higher speeds - only WMM Advertise should be disabled	WMM No Acknowledgement: Disabled
WMM No Acknowledgement	Disabled - some devices may not support this	WMM APSD: Enabled
WMM APSD	This is a WMM Power save that replaces the RX Chain power save options	

1.D Select the **“Save/Apply”** Button.

Section 10.5- MAC FILTERING

When to MAC Filtering

MAC Filtering is not a security measure, and does not replace encryption. Even with MAC Filtering you can sniff packets for review; and MAC Addresses can be spoofed.

MAC Address filtering, however, can help to minimize the effects of unwanted requests, and the connection of average users.

Step 1: Direct Your Browser to the MAC Filter Page

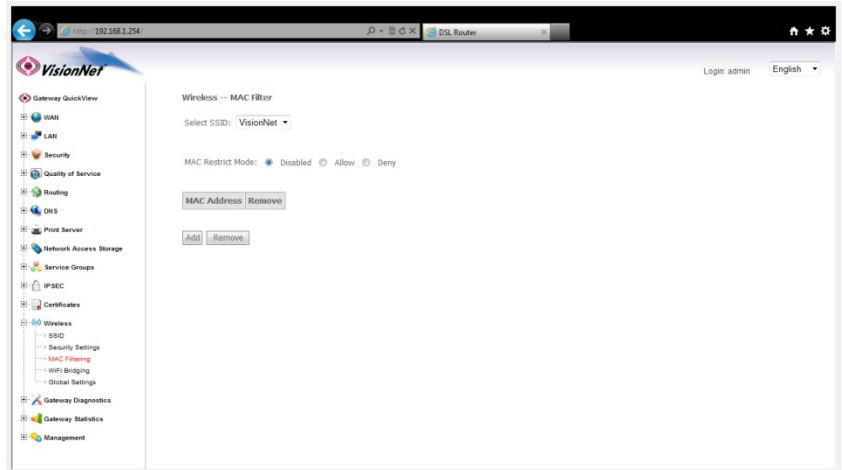
- 1.A Select the **“Wireless”** tab located within the left-hand frameset.

Then, in the left-hand frameset, select **“MAC Filtering”**

Allow: Means that only the specified MACs are allowed

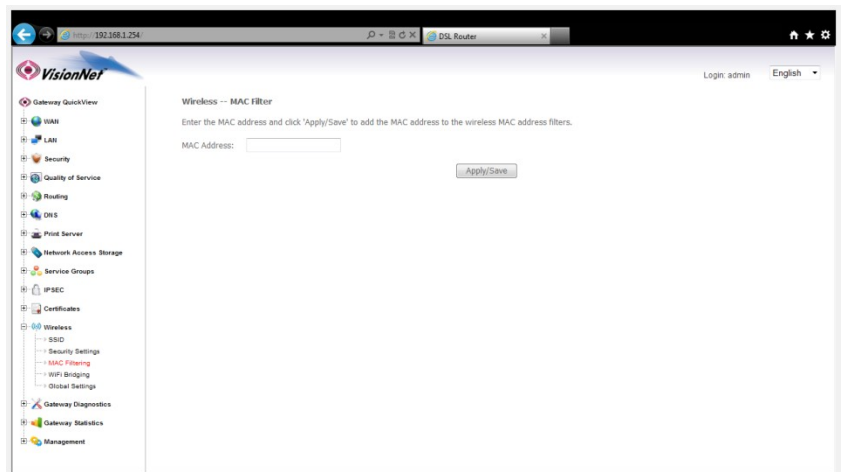
Deny: Means that the specified MAC Addresses are not allowed access

Disabled: Means that the MAC Filtering table is not applied



- 1.B Select the appropriate SSID, and then select Add

You may now add a MAC Address to be filtered



Section 10.6 - Wireless Bridge

What is Wireless Bridge

Wireless Bridge allows an AP to connect to another AP to rebroadcast the network

Step 1: Direct Your Browser to the Wireless Bridge Page

1.A Select the **“Wireless”** tab located within the left-hand frameset.; then select **“Wireless Bridging”**

Then, in the left-hand frameset, select **“MAC Filtering”**

AP Mode

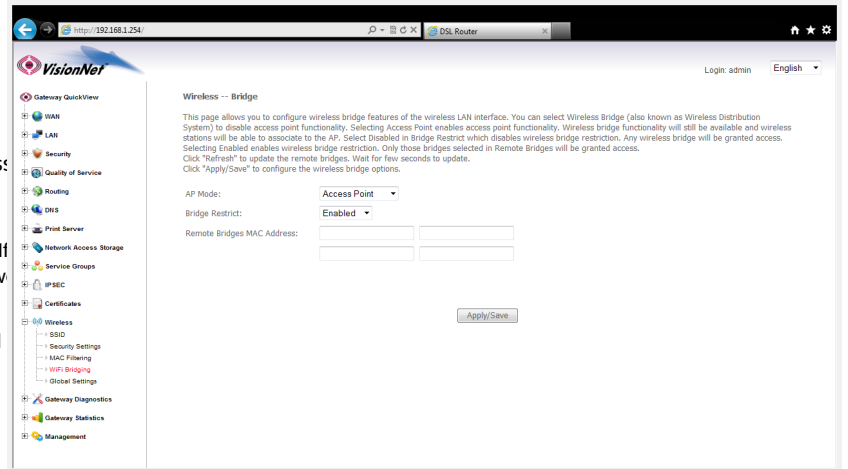
Select Wireless Bridge or Access Point

Bridge Restrict

Disabled if you are using Bridging; If enabled other APs will not be allowed to connect

Remote Bridges

The MAC Addresses of the allowed Remote Bridges

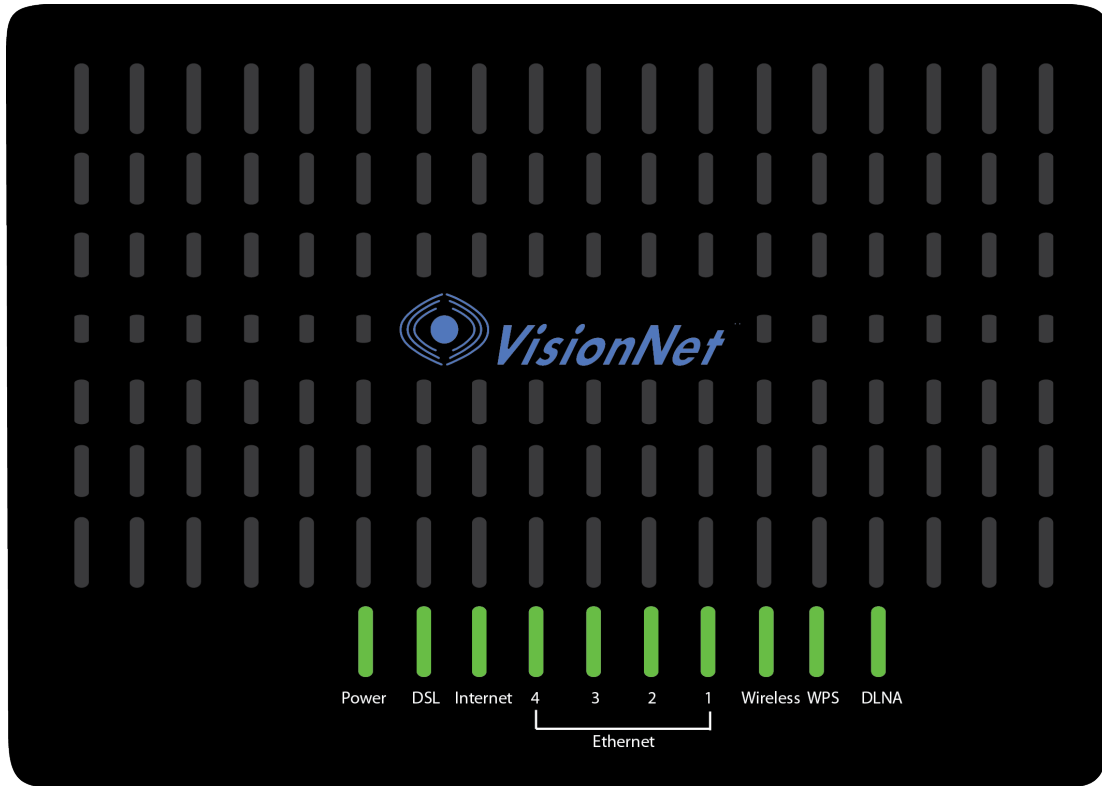


1.B Select **“Apply / Save”**

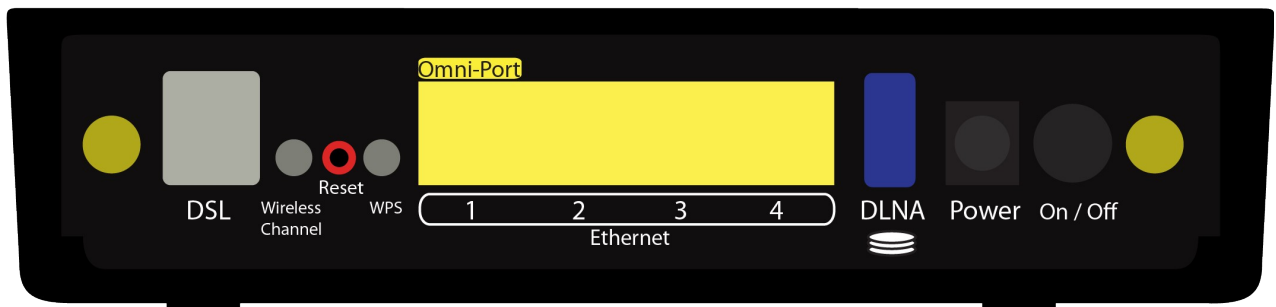
SECTION 11: PRODUCT DEPICTIONS AND BEHAVIOR

Section 11.1 - Product Depictions

M505N LED VIEW



M505N REAR VIEW



Section 11.2 - LED Behavior

LED Label	Purpose	Location	Color/Behavior
Power	Status Power/ Router	Front	<p>Solid Green – Power On</p> <p>Off – Power Off</p> <p>Flashing Red – Flashing Power on self test</p> <p>Solid Red - Failure (not bootable) or device malfunction <i>A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data. This may be identified at various times such as after power on or during operation through the use of self testing or in operations which result in a unit state that is not expected or should not occur.</i></p>
Ethernet 1	Status Ethernet Port	Front	<p>Off - Power Off – or – No Powered device detected</p> <p>Solid Green – Powered device connected ; including wake on LAN</p> <p>Flashing Green – LAN activity present for that port</p>
Ethernet 2	Status Ethernet Port	Front	<p>Off - Power Off – or – No Powered device detected</p> <p>Solid Green – Powered device connected ; including wake on LAN</p> <p>Flashing Green – LAN activity present for that port</p>
Ethernet 3	Status Ethernet Port	Front	<p>Off - Power Off – or – No Powered device detected</p> <p>Solid Green – Powered device connected ; including wake on LAN</p> <p>Flashing Green – LAN activity present for that port</p>
Ethernet 4	Status Ethernet Port	Front	<p>Off - Power Off – or – No Powered device detected</p> <p>Solid Green – Powered device connected ; including wake on LAN</p> <p>Flashing Green – Activity present for that port</p>
DLNA	Status USB Port	Front	<p>Off - Power Off – or – No Device detected</p> <p>Solid Green – Device connected</p> <p>Flashing Green – Activity present on port</p>
Wireless	Status Wireless	Front	<p>Off - Modem off or Wireless not activated</p> <p>Solid Green – Wireless activated</p> <p>Flashing Green – Wireless activity is present</p>
DSL	Status DSL	Front	<p>Green – DSL Good Sync</p> <p>Off – Powered off</p> <p>Flashing Green - DSL Attempting sync <i>Signal Detection – Flashing 2hz with 50% duty cycle</i> <i>Carrier Detected, Modem training – Flashing at 4hz with 50% duty cycle</i></p>
Internet	Status WAN	Front	<p>Internet Light – Must indicate at least one type of connection</p> <p>Solid Green – IP connected – no traffic passing Device has a WAN IP via either static/ DHCP/ or IPCP If PPP is used, device has authenticated and has a WAN IP Address If IP or PPPOE session is idle and dropped, light to remain green as long as ADSL is still present. <i>Light to turn red if upon attempting new session it fails.</i></p> <p>Off – Modem Power Off. LED Should remain off if modem is in bridged mode or if DSL Connection is not present</p> <p>Flashing Green – Device has WAN IP Address and IP Traffic is passing through device</p> <p>Red – Device attempted initiate session, either authentication or to obtain an IP Address, and failed.</p>

Section 12.1 - Port Mirroring

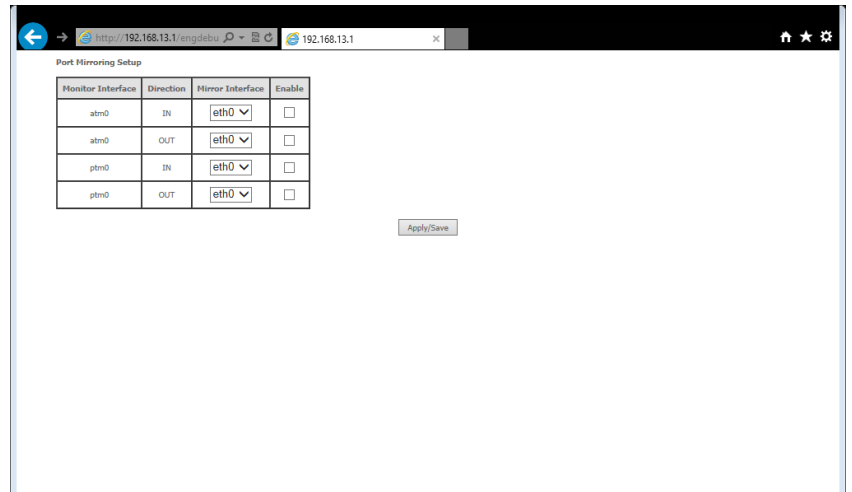
Port Mirroring will allow for complete packet captures when using a capture application such as WinPCAP or tcpdump.

Mirroring a WAN port will duplicate WAN packets to the first Ethernet Port for technicians to view.

Step 1: Access the GUI to find Backup Configuration Tool

- 1.A In your browser, go to : <http://192.168.x.x/engdebug.cmd>

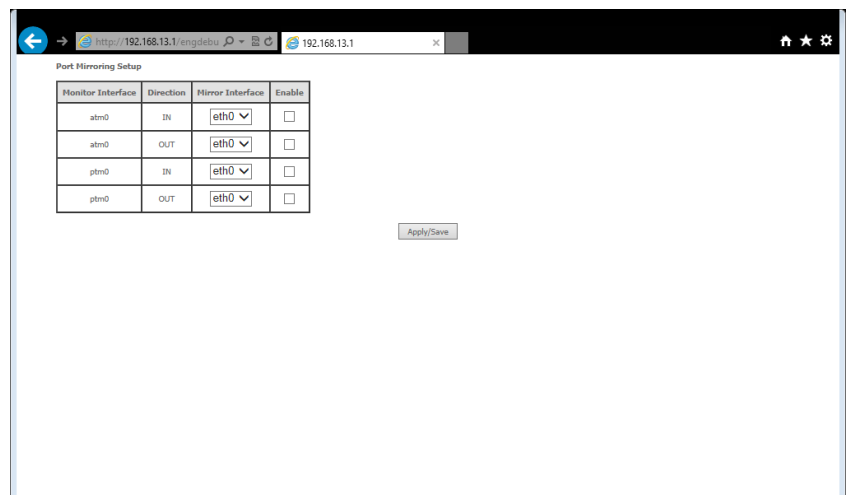
Then, enable “In” and “Out”
(Ingress and Egress packets) for the
appropriate WAN interface



- 2.A Select the Ethernet Port for Mirroring

Please note that number begins
with “O”. Hence

Eth0 = Port 1
Eth1 = Port 2
Eth2 = Port 3



- 3.A Select “Apply / Save” .