# Product Manual

# Model: M504 / M505N R3

# Product Description:  Broadband Gateway

| | |
|---|---|
| **WAN:** | **ADSL2+ / Ethernet WAN** |
| **Ethernet:** | **Qty 4 - 10/100 Ethernet** |
| **USB:** | **2.0 (Media Share / Wireless Uplink)** |
| **WiFi:** | **802.11 b/g/n 2T2R 2.4Ghz with Internal Airgain Antenna** |

**Manual Version: 0.1c**
**Manual Date: July 2014**

**Table of Contents**

## SECTION 7: IPv4 DNS CONFIGURATION

## SECTION 8: IPv4 NAT TRAVERSAL

## SECTION 9: WIFI CONFIGURATION

## SECTION 10: PRODUCT SPECIFICATION

This page intentionally left blank

This page intentionally left blank

# SECTION 1: MANAGEMENT ACCESS

## SECTION 1.1 UNDERSTANDING YOUR DOCUMENTATION

**Item 1** **Obtaining the most recent documentation from your VisionNet Sales Engineer**

Only pre-approved ILEC/CLEC representatives may receive documentation . If you are not recognized on that list, please ask the authorized company representative to add you to our list.

**Item 2** **You will receive the following files:**

| | |
|---|---|
| **Configuration File** | This is the generic xml file, used at the time of customization, sans device unique parameters |
| **Customer Configuration Form** | This is the explanatory form that summarizes the contents of the configuration, and includes passwords in plain-text.<br>This form should only be distributed to authorized employees |
| **Optional: Logo** | The VisionNet Logo may be replaced by a custom .png or gif file |
| **Optional: DNS Redirect Branding** | The custom DNS Redirect, used for DSL Sync and PPP Troubleshooting, may be over-written with a custom html file including contact information and instructions. |

**Item 3** **Types of configurations kept for records:**

| | |
|---|---|
| **Shipping Configurations** | These configurations are approved for shipping, and may be referenced by POs, for use. Shipping configuration changes must be requested by authorized technical representatives |
| **Alternate Configurations** | These configurations are not used for shipping, but are recognized as approved for deployment. These may be provided to technicians upon request. |
| **Testing Configurations** | These configurations are not used for shipping, or recognized for deployment. They are for testing, development, or are being considered for final approval. |

# SECTION 1.2 MANAGEMENT ACCOUNTS

## Item 1 Management Accounts

It has been common practice, in the past, for in-field technicians, and lower level remote support, to receive full admin access.

As of “Solution Suite 3” , 5 accounts are utilized for department appropriate access to VisionNet modems.

## Item 2 Security Advisory

**Strict adherence to the following account access restrictions is advised:**

| | |
|---|---|
| **High Level Access** | Limited to Engineering and NOC departments |
| **Medium Level Access** | Limited to in-field technicians and ISP employed customer support |
| **Low Level Access** | ONLY THIS LEVEL ACCESS SHOULD BE PROVIDED TO END USERS |

## Item 3 Types of configurations kept for records:

| Access | Account Name | GUI Privilege | CLI Privilege |
|---|---|---|---|
| Local | engineering | High | High |
| Local | technician | Medium | Medium |
| Local | enduser | Low | None |
| Remote | networkops | High | High |
| Remote | techsupport | Medium | Medium |

# SECTION 1.3 SERVICE SECURITY CONSIDERATIONS

## Item 1 Default use of Non-Standard Ports

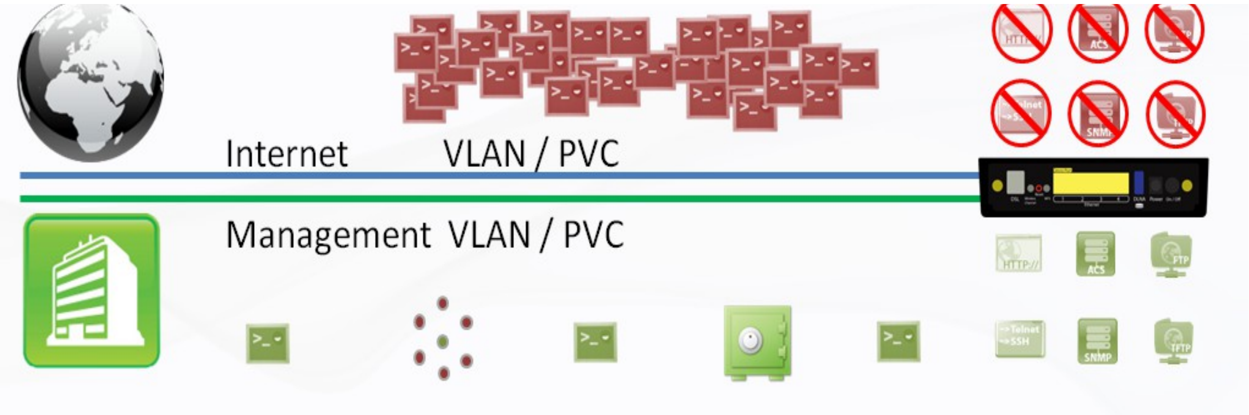
Use of Non-Standard ports help ensure consistency in an environment where UPnP, and customer port forwarding, may re-map standard ports for personal use.

The following ports are used as VisionNet defaults:

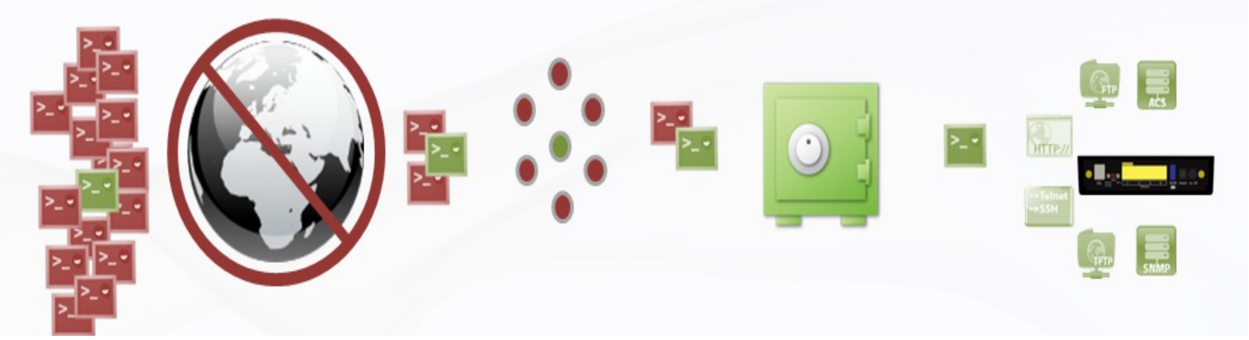
| Service | LAN Port / Status | WAN Port - Status |
|---|---|---|
| HTTP | 80 - Enabled | 6080 - Enabled |
| TELNET | 23 - Enabled | 6023 - Disabled |
| SSH | 22 - Enabled | 6022 - Enabled |
| FTP | 21 - Disabled | 21 - Disabled |
| TFTP | 69 - Enabled | 69 - Disabled |
| ICMP | N/A - Enabled | N/A - Enabled |
| SNMP | 161 - Disabled | 161 - Disabled |
| SAMBA | 445 - Enabled | N/A |

## Item 2 WAN Interface Restrictions

**Dedicated PVC / VLANs are an effective method of isolating management services to privately managed networks; thus removing potential security threats.**



**IP based ACLs are suggested for public facing WAN services.**



## SECTION 1.4 GUI ACCESS

### STEP 1 Verify IP Information

1.A Determine the IP and Port of the service interface.

**If you are accessing the unit remotely:**

Determine the WAN IP and Service Port.

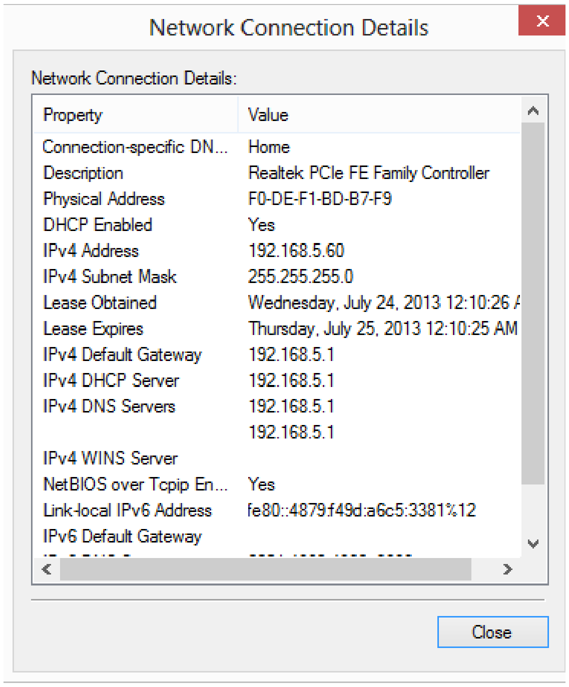
Verify that your local IP will not be blocked by any gateway, or network, ACLs.

**If you are accessing the unit locally:**

Determine the LAN IP of the gateway.

In a NAT, or Routed configuration, this will be your Gateway IP, assigned by DHCP.

In a Bridged configuration, you will need to statically assign an IP, to your device, within the same subnet as the gateway's unadvertised LAN IP.



Network Connection Details

Network Connection Details:

| Property | Value |
|---|---|
| Connection-specific DN... | Home |
| Description | Realtek PCIe FE Family Controller |
| Physical Address | F0-DE-F1-BD-B7-F9 |
| DHCP Enabled | Yes |
| IPv4 Address | 192.168.5.60 |
| IPv4 Subnet Mask | 255.255.255.0 |
| Lease Obtained | Wednesday, July 24, 2013 12:10:26 A |
| Lease Expires | Thursday, July 25, 2013 12:10:25 AM |
| IPv4 Default Gateway | 192.168.5.1 |
| IPv4 DHCP Server | 192.168.5.1 |
| IPv4 DNS Servers | 192.168.5.1<br>192.168.5.1 |
| IPv4 WINS Server | |
| NetBIOS over Tcpip En... | Yes |
| Link-local IPv6 Address | fe80::4879:f49d:a6c5:3381%12 |
| IPv6 Default Gateway | |

### Step 2 Connect via Web Browser

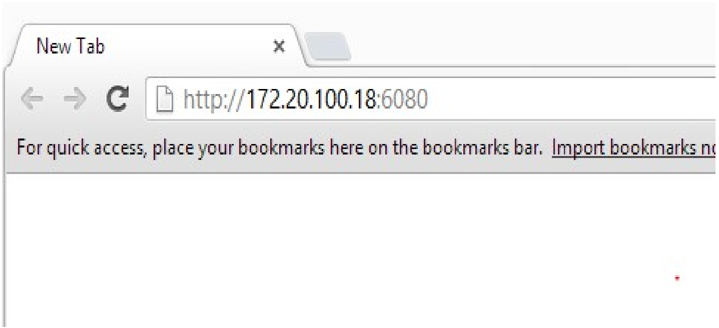
2.A In your browser's address bar, enter the IP Address and, if remote, port number used for access.

**Example of WAN Access:**

http://172.20.100.18:6080

**Example of LAN Access:**

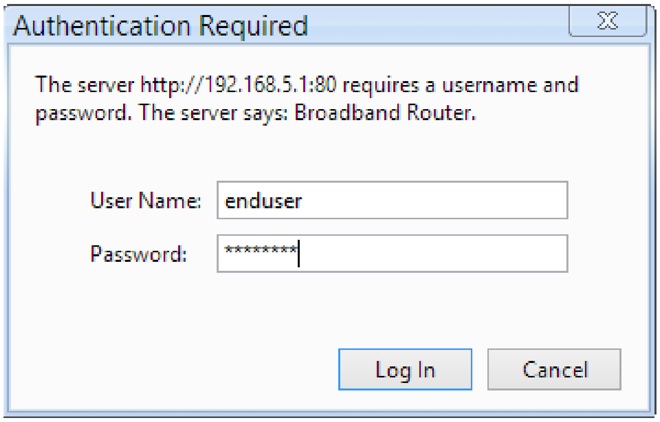
http://192.168.6.1



http://172.20.100.18:6080

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks n

2.B When Challenged, enter the username and password associated with your account.



Authentication Required

The server http://192.168.5.1:80 requires a username and password. The server says: Broadband Router.

User Name: enduser

Password: ********

# SECTION 1.5 CLI ACCESS

## STEP 1 Verify IP Information

1.A Determine the IP and Port of the service interface.

**If you are accessing the unit remotely:**

Determine the WAN IP and Service Port.

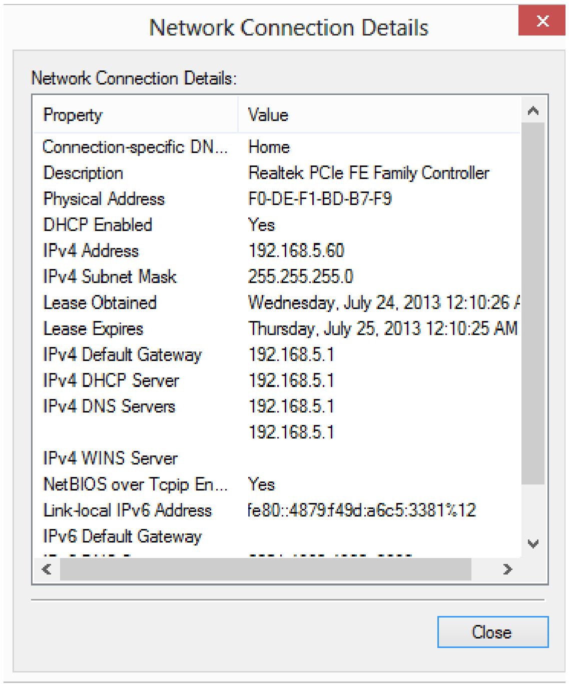
Verify that your local IP will not be blocked by any gateway, or network, ACLs.

**If you are accessing the unit locally:**

Determine the LAN IP of the gateway.

In a NAT, or Routed configuration, this will be your Gateway IP, assigned by DHCP.

In a Bridged configuration, you will need to statically assign an IP, to your device, within the same subnet as the gateway's unadvertised LAN IP.



Network Connection Details:

| Property | Value |
|---|---|
| Connection-specific DN... | Home |
| Description | Realtek PCIe FE Family Controller |
| Physical Address | F0-DE-F1-BD-B7-F9 |
| DHCP Enabled | Yes |
| IPv4 Address | 192.168.5.60 |
| IPv4 Subnet Mask | 255.255.255.0 |
| Lease Obtained | Wednesday, July 24, 2013 12:10:26 A |
| Lease Expires | Thursday, July 25, 2013 12:10:25 AM |
| IPv4 Default Gateway | 192.168.5.1 |
| IPv4 DHCP Server | 192.168.5.1 |
| IPv4 DNS Servers | 192.168.5.1 |
|  | 192.168.5.1 |
| IPv4 WINS Server |  |
| NetBIOS over Tcpip En... | Yes |
| Link-local IPv6 Address | fe80::4879:f49d:a6c5:3381%12 |
| IPv6 Default Gateway |  |

## Step 2 Connect via Client

2.A Via your OS Terminal, or Console Program, you may enter the IP and Port information

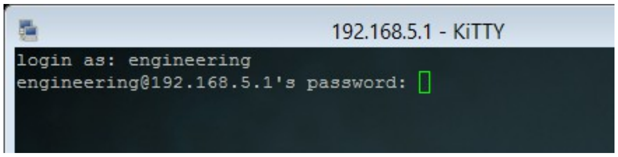
**Example of WAN Access:**

172.20.100.18 port 6022

**Example of LAN Access:**

192.168.6.1 port 22

2.B When Challenged, enter the username and password associated with your account.



```
login as: engineering
engineering@192.168.5.1's password: 
```

# SECTION 2: WAN CONFIGURATION

## SECTION 2.1 WAN LOGIC OVERVIEW

**Item 1 OSI RELATION**

### 1.A WAN IF (Interfaces)

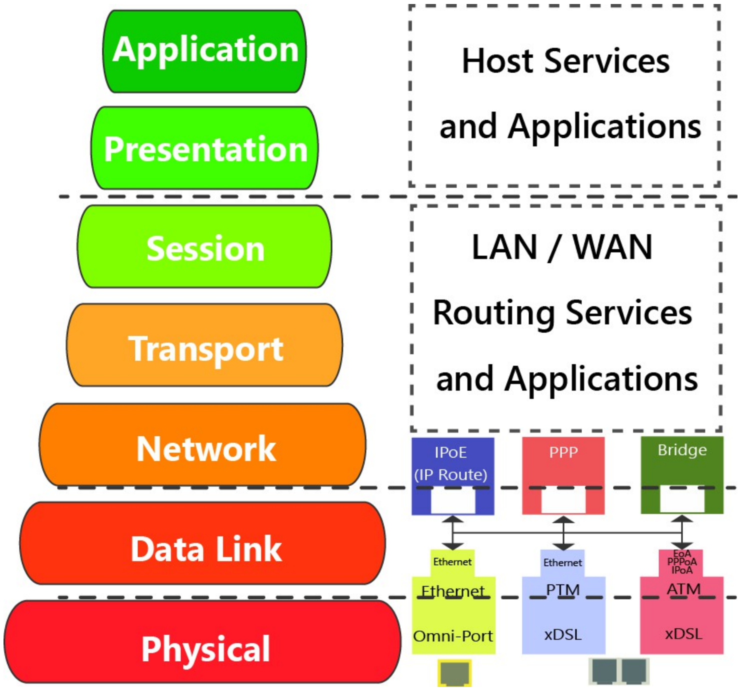
There are three possible “Layer 1 – 2” WAN Configurations Available

**ATM**
**Available for: xDSL Interface**
*Most Commonly Associated with ADSL*

**PTM**
**Available for: xDSL Interface**
*Most Commonly Associated with VDSL2*

**ETH**
**Available for: Omni-Port WAN Interface**
*Building This Interface Removes the “Omni-Port” from LAN Operation*

**Configured Here:**
Physical WAN Interfaces Used, Data Link, VLAN Mux, QoS, ATM PVC’s, ATM Non-Ethernet Services.



### 1.B WAN Services

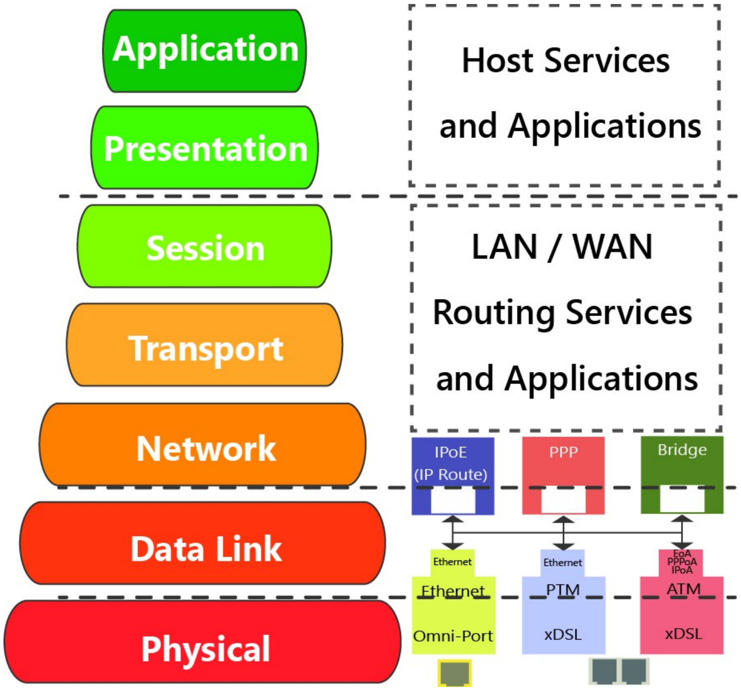
There are three possible “Layer 2 – 3” WAN Configurations Available

**Bridged**
**Available for: ATM, PTM, ETH**
*Passes Traffic – No Routing*

**IPoE**
**Available for: ATM, PTM, ETH**
*Routing, WAN Clients (DHCP, RADVD, ETC), Firewall Type, NAT, Proxies*

**PPP**
**Available for: ATM, PTM, ETH**
*PPP Client, Routing, WAN Clients (DHCP, RADVD, ETC), Firewall Type, NAT, Proxies*

**Configured Here:**
Service Type, VLAN Tagging, Routing Services, IP Services, WAN Clients and Proxies



## Item 2 WAN Creation / Deletion

### 2.A Building WAN Services

WAN Services Must be added as follows

**1: Add & Define WAN Interface**
ATM
PTM
ETH (Omni-Port)

**2: Add and Define Service to Interface**
ATM
PTM
ETH (Omni-Port)

**3: Prioritize for Default Service Group**
Gateway
DNS

**4: Add Service Group**
If Applicable

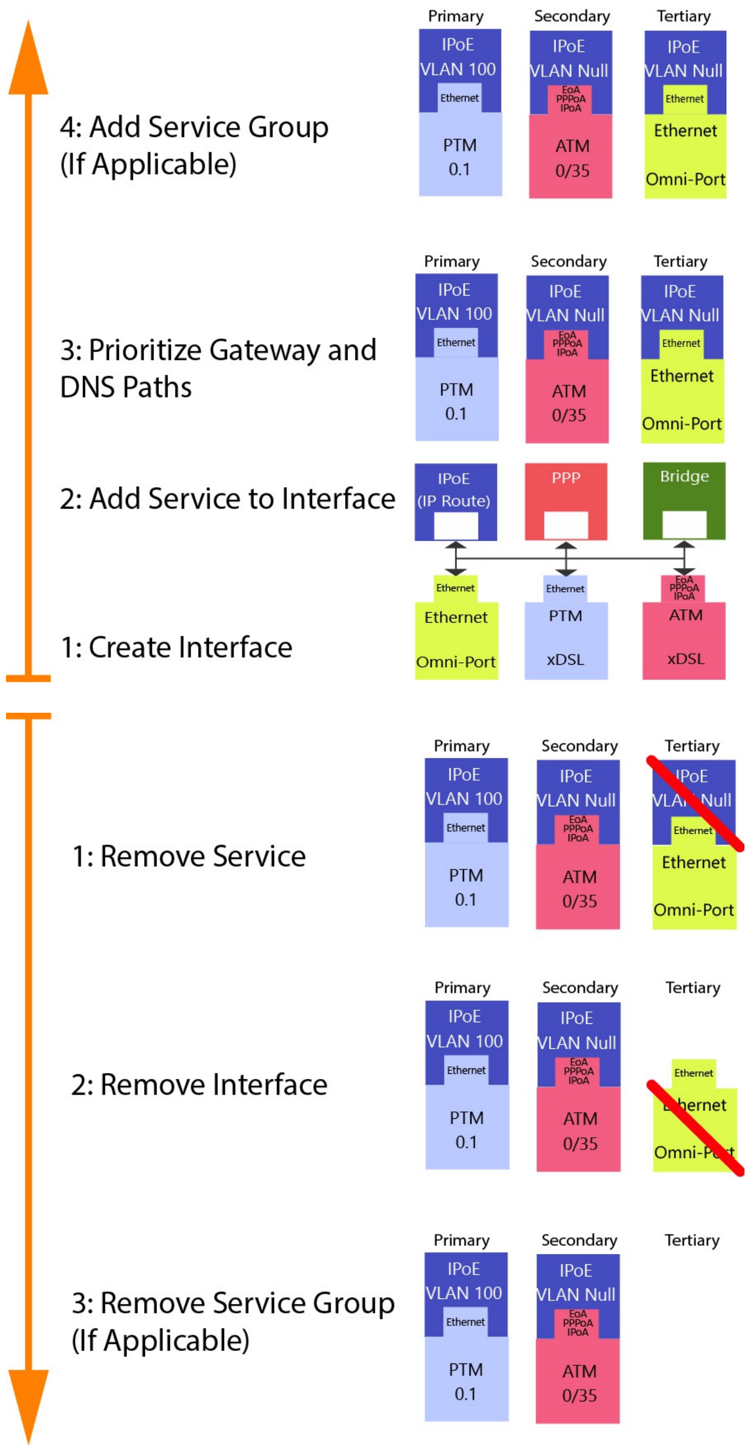
### 2.B Tearing Down WAN Services

WAN Services Must be removed as follows:

**1: Remove WAN Service**
This must be removed first

**2: Remove Interface**
This may not be removed unless all associated WAN Services are removed

**3: Remove Service Group**
Remaining Group Interfaces will not be ungrouped by default



## Item 3 Physical Port Prioritization

### 3.1 There are three Physical WAN Options

#### xDSL Operation

This operation only allows the xDSL port to be used for WAN operation.

This will not convert the “Omni-Port” to LAN mode if an “ETH” Interface is enabled

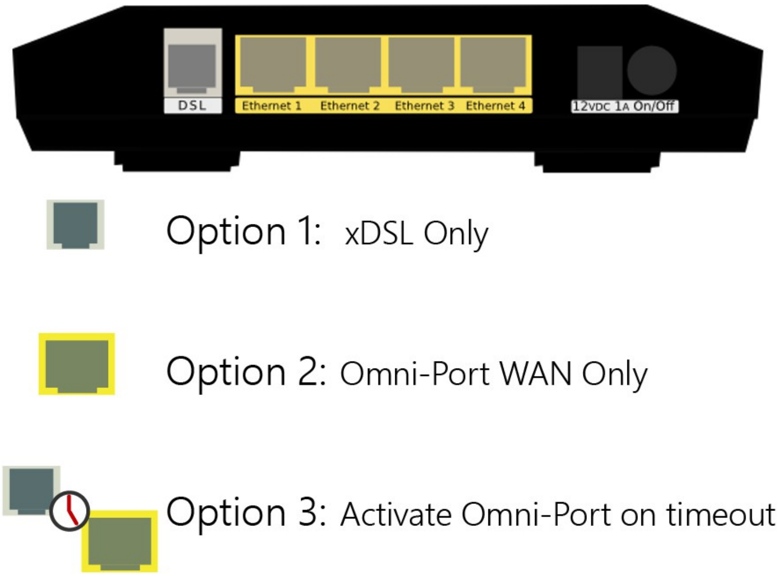
#### Omni-Port WAN Operation

This operation only allows WAN Service through the Omni-Port.

This will not remove created xDSL Services

#### WAN Time-out Operation

If xDSL signal is not detected, within a specified amount of time (default 120 seconds), the created Omni-Port WAN Interface will be activated.

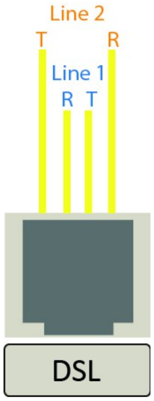


# SECTION 2.2 x DSL LOGIC

## Item 1 x DSL Physical Interfaces

### 1.A xDSL Port Layout

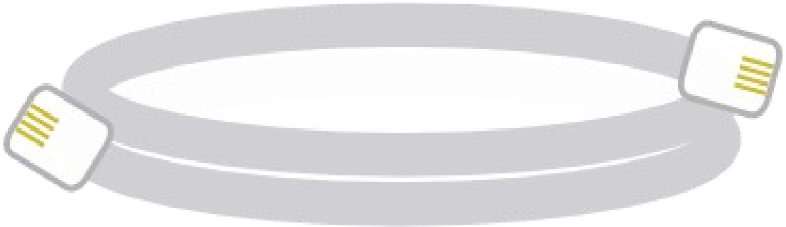
**Line Pinout**



The CPE is designed to operate on one line 1 Only.

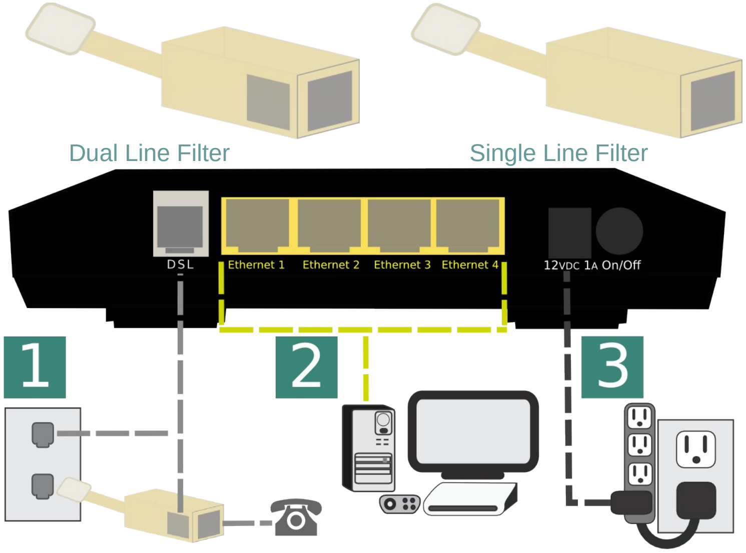
### 1.B xDSL Line Cord Preferences

VisionNet provides a standard xDSL cable



## Item 2 Physical Installation

**2.A** Filters may be provided by VisionNet, or provided by a 3rd party to your company



2.B 1) Connect DSL

DSL May be connected directly to wall jack

A dual port filter may be used as well.

2) Connect Ethernet Devices

Ethernet is suggested for gaming consoles, servers, and other synchronous, latency dependent, applications

3) Connect Power

Connect power to Surge Protector

The over-voltage protection in the provided PSU is not designed to replace a proper surge protector.

## 2.B ADSL2+

### ADSL – ADSL2+

**Operating Frequency:**
20 Khz – 2.2 Mhz

**MaxSpeed:**
24Mbps DS, 2.2Mbps US

**General Operation:**
ATM (PTM on some CO equipment)

| Standard | ITU Standard | Max Frequency (Mhz) |
|---|---|---|
| **ADSL** | G.992.1 | 1.1 |
| **ADSL2** | G.992.3 | 1.1 |
| **ADSL2+** | G.992.5 | 2.2 |

## Item 3 xDSL Properties

**Below, is a brief summary of some xDSL protocols to familiarize yourself with:**

| Class | Protocol | Standard | Notes |
|---|---|---|---|
| ADSL | G.DMT | ITU G.992.1 | 8Mbps DS / 1.3 Mbps US |
| ADSL | G.Lite | ITU G.992.2 | 1.5 Mbps DS / 512 kbps US |
| ADSL | T1.413 | ANSI T1.413 | 8Mbps DS / 1.3 Mbps US |
| ADSL2 | ADSL2 | ITU G.992.3 | 12 Mbps DS / 800 kbps US |
| ADSL2 | Annex L | ITU G.992.3 | Increases ADSL2 Reach to 7 km (23k ft) |
| ADSL2+ | ADSL2+ | ITU G.992.5 | Doubles Frequency Range from 1.1Mhz to 2.2 Mhz. |
| ADSL2+ | Annex M | ITU G.992.5 | Changes DS / US frequency split, to double US to max 3.3 Mbps |
| Capability | Bitswap | ITU G.992.1 | Allows for movement of bit transmission between "bins" |
| Capability | SRA | ITU G.992.5 | ADSL2+: Allows for rate changes without re-training |
| Capability | Trellis | Multiple | Modulation Scheme Rate / Reach performance improvement |
| Capability | PhyR | Proprietary | ADSL2+: Physical Layer ReTransmission - Broadcom support only |
| Capability | Interleave | ITU G709 | Forwarding Error Correction / delay preferred <5ms |

# SECTION 2.3 CUSTOMIZING xDSL PARAMETERS

**Abstract**

This section will provide instructions on changing xDSL parameters. Upon changing parameters, your modem will need to re-train; and you will be temporarily disconnected from WAN side connections.

This section will not explain, in detail, the various ATM based options; these should be specified by an ISPs Network Operations Center and OSP Manager.

**Step 1 Direct your browser to the xDSL Properties page**

**1.A** In the left-hand navigation pane, select:

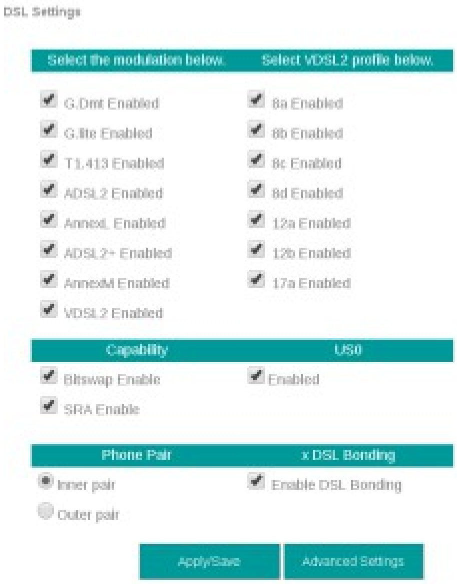
**WAN**

**xDSL Properties**

**Step 2 Select the appropriate parameters for xDSL configuration**

**2.A Select Parameters**

The necessary parameters will be dictated by your network, DSLAM capabilities, and profile considerations
**xDSL Properties**



DSL Settings

| Select the modulation below. | Select VDSL2 profile below. |
|---|---|
| ☑ G.Dmt Enabled | ☑ 8a Enabled |
| ☑ G.lite Enabled | ☑ 8b Enabled |
| ☑ T1.413 Enabled | ☑ 8c Enabled |
| ☑ ADSL2 Enabled | ☑ 8d Enabled |
| ☑ AnnexL Enabled | ☑ 12a Enabled |
| ☑ ADSL2+ Enabled | ☑ 12b Enabled |
| ☑ AnnexM Enabled | ☑ 17a Enabled |
| ☑ VDSL2 Enabled | |

| Capability | US0 |
|---|---|
| ☑ Bitswap Enable | ☑ Enabled |
| ☑ SRA Enable | |

| Phone Pair | x DSL Bonding |
|---|---|
| ● Inner pair | ☑ Enable DSL Bonding |
| ○ Outer pair | |

**2.B** Select “Save / Apply”

# SECTION 2.4 DEFINING PHYSICAL WAN PORT OPERATION

**Abstract**

This section will provide instruction in specifying the physical Port used for WAN Service

**Step 1 Direct your browser to the WAN IF: Services page**

1.A In the left-hand navigation pane, select:

**WAN**

**WAN IF: Services**

**Step 2 Select the appropriate parameters for WAN Interface Selection**

**2.A xDSL Interface:**

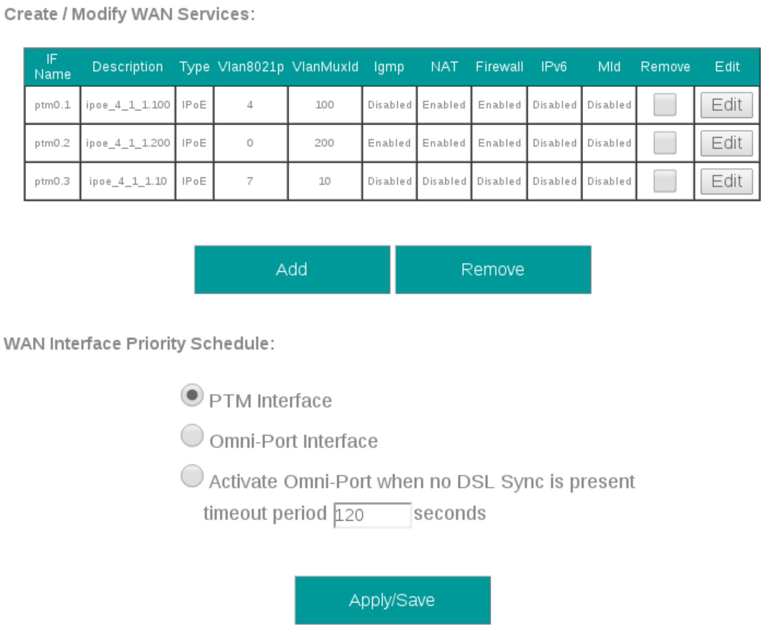
In some FW Revisions, this is labeled PTM. ATM is also supported in this mode.

**Omni-Port Interface**

An Ethernet interface and service must be created

**Time-out**

Enable Omni-Port, when no DSL Sync is present,  within specified time after boot-up.



Create / Modify WAN Services:

| IF Name | Description | Type | Vlan8021p | VlanMuxId | Igmp | NAT | Firewall | IPv6 | Mld | Remove | Edit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ptm0.1 | ipoe_4_1_1.100 | IPoE | 4 | 100 | Disabled | Enabled | Enabled | Disabled | Disabled | □ | Edit |
| ptm0.2 | ipoe_4_1_1.200 | IPoE | 0 | 200 | Enabled | Enabled | Enabled | Disabled | Disabled | □ | Edit |
| ptm0.3 | ipoe_4_1_1.10 | IPoE | 7 | 10 | Disabled | Disabled | Disabled | Disabled | Disabled | □ | Edit |

WAN Interface Priority Schedule:

● PTM Interface

○ Omni-Port Interface

○ Activate Omni-Port when no DSL Sync is present

timeout period 120 seconds

2.B Select "Save / Apply"

# SECTION 2.5 CREATING AN ATM INTERFACE

**Abstract**

This section will demonstrate the creation of an ATM Interface, most commonly used for ADSL/2/2+ Operation.

This section will not explain, in detail, the various ATM based options; as this must be specified by an ISPs Network Operations Center and OSP Manager.

**Step 1 Direct your browser to the WAN IF: ATM page**

**1.A** In the left-hand navigation pane, select:

**WAN**

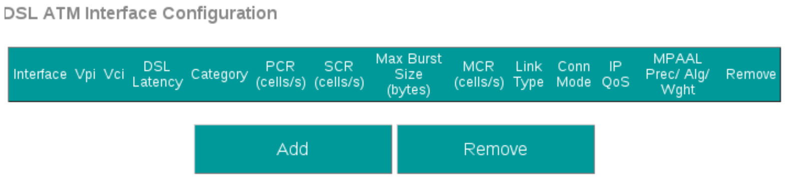
**WAN IF: ATM**

**Step 2 Create an ATM Interface**

**2.A** **Select "Add"**

**Notes:**
You must remove, and rebuild, an interface if you would like to change parameters.

Associated WAN Services must be removed, before an interface may be removed.



DSL ATM Interface Configuration

| Interface | Vpi | Vci | DSL Latency | Category | PCR (cells/s) | SCR (cells/s) | Max Burst Size (bytes) | MCR (cells/s) | Link Type | Conn Mode | IP QoS | MPAAL Prec/ Alg/ Wght | Remove |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

## 2.B Modify Parameters

**Notes:**

**VPI/VCI**
If you are using more than one vlan, create one PVC. The VLANs will be added during WAN Service configuration.

**DSL Latency**
If “Interleave” (PATH 1) is to be selected, “Fast” (PATH 0) must also be selected

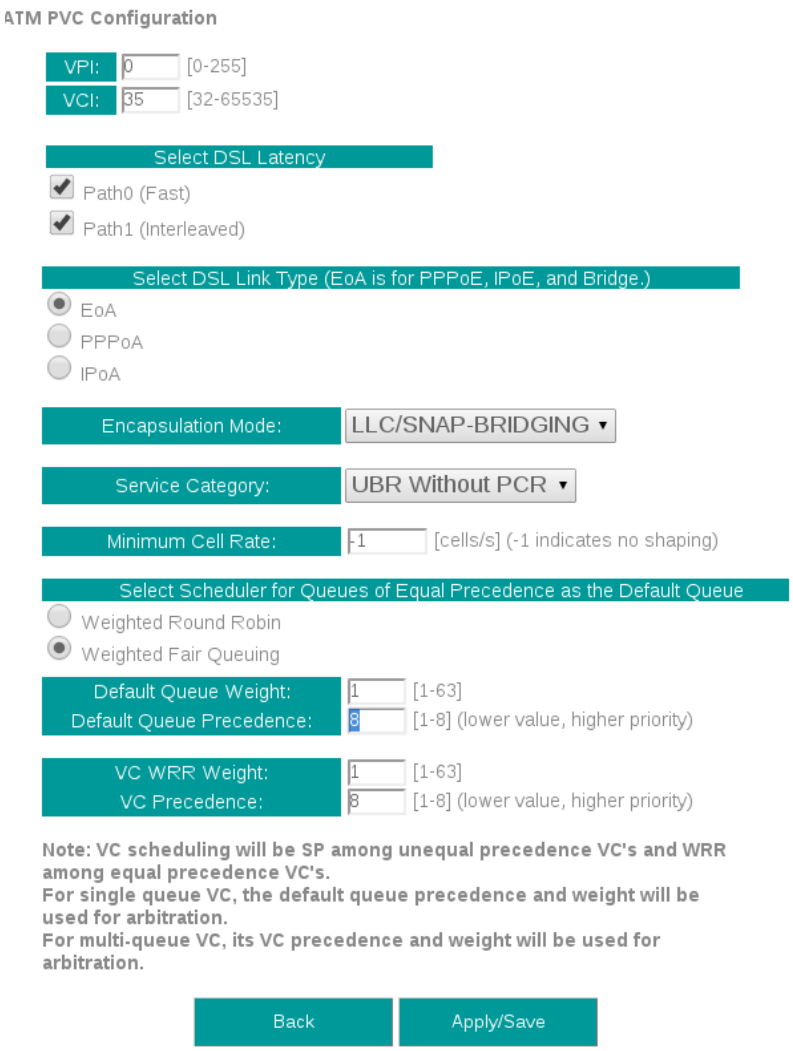
**DSL Link Type**
EoA (Ethernet over ATM)will be used for all Ethernet based Bridge, PPP, and IP Services; PPPoA and IPoA are exclusively ATM based

**Encapsulation Mode**
Default: LLC/Snap-Bridging

**Service Category**
Default: UBR without PCR

**Minimum Cell Rate:**
Default : -1

**QoS Scheduler**
Select WRR or WFQ
You may select Queue Weight and Precedence for the ATM.
This will affect QoS Prioritization for upstream traffic only.



ATM PVC Configuration

VPI: 0 [0-255]
VCI: 35 [32-65535]

Select DSL Latency
☑ Path0 (Fast)
☑ Path1 (Interleaved)

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
● EoA
○ PPPoA
○ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

Minimum Cell Rate: -1 [cells/s] (-1 indicates no shaping)

Select Scheduler for Queues of Equal Precedence as the Default Queue
○ Weighted Round Robin
● Weighted Fair Queuing

Default Queue Weight: 1 [1-63]
Default Queue Precedence: 8 [1-8] (lower value, higher priority)

VC WRR Weight: 1 [1-63]
VC Precedence: 8 [1-8] (lower value, higher priority)

Note: VC scheduling will be SP among unequal precedence VC's and WRR among equal precedence VC's.
For single queue VC, the default queue precedence and weight will be used for arbitration.
For multi-queue VC, its VC precedence and weight will be used for arbitration.

## 2.C Select “Apply / Save”

# SECTION 2.6   CREATING A PTM INTERFACE

**Abstract**

This section will demonstrate the creation of a PTM Interface, most commonly used for VDSL2 Operation.

This section will not explain, in detail, the various PTM based options; as this must be specified by an ISPs Network Operations Center and OSP Manager.

**Step 1  Direct your browser to the WAN IF: PTM page**

**1.A** In the left-hand navigation pane, select:

**WAN**

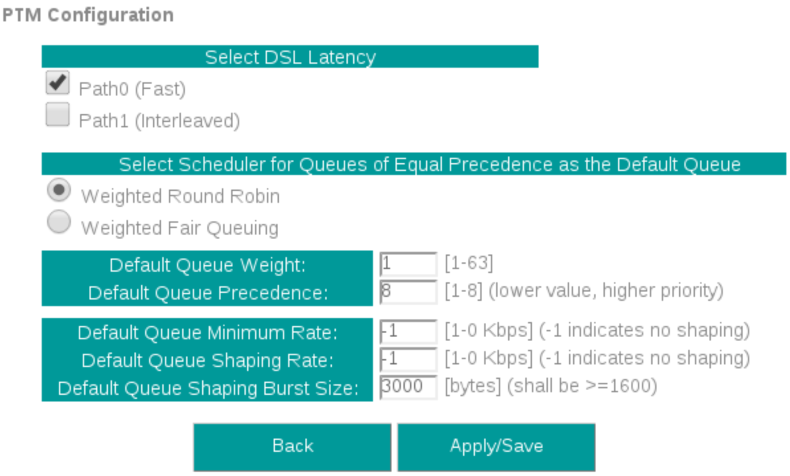
**WAN IF: PTM**

**Step 2  Create a PTM Interface**

**2.A Select “Add”**

**Notes:**
You must remove, and rebuild, an interface if you would like to change parameters.

Associated WAN Services must be removed, before an interface may be removed.



PTM Configuration

Select DSL Latency

☑ Path0 (Fast)

□ Path1 (Interleaved)

Select Scheduler for Queues of Equal Precedence as the Default Queue

● Weighted Round Robin

○ Weighted Fair Queuing

Default Queue Weight: 1 [1-63]

Default Queue Precedence: 8 [1-8] (lower value, higher priority)

Default Queue Minimum Rate: -1 [1-0 Kbps] (-1 indicates no shaping)

Default Queue Shaping Rate: -1 [1-0 Kbps] (-1 indicates no shaping)

Default Queue Shaping Burst Size: 3000 [bytes] (shall be >=1600)

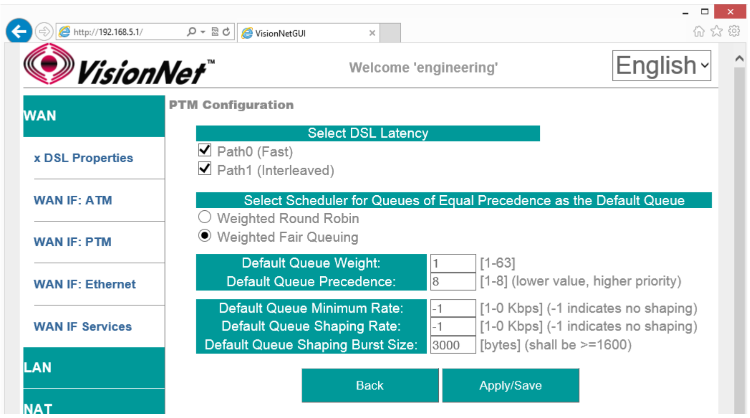
**2.B Modify Parameters**

**Notes:**

**VLAN MUX**
VLAN MUX is enabled by default.

**DSL Latency**
If “Interleave” (PATH 1) is to be selected, “Fast” (PATH 0) must also be selected

**QoS Scheduler**
Select WRR or WFQ
You may select Queue Weight and Precedence for the ATM.
This will affect QoS Prioritization for upstream traffic only.



PTM Configuration

Select DSL Latency

☑ Path0 (Fast)

☑ Path1 (Interleaved)

Select Scheduler for Queues of Equal Precedence as the Default Queue

○ Weighted Round Robin

● Weighted Fair Queuing

Default Queue Weight: 1 [1-63]

Default Queue Precedence: 8 [1-8] (lower value, higher priority)

Default Queue Minimum Rate: -1 [1-0 Kbps] (-1 indicates no shaping)

Default Queue Shaping Rate: -1 [1-0 Kbps] (-1 indicates no shaping)

Default Queue Shaping Burst Size: 3000 [bytes] (shall be >=1600)

**2.C** Select “Apply / Save”

# SECTION 2.7  CREATING AN ETHERNET INTERFACE

**Abstract**

This section will demonstrate the creation of an Ethernet nterface, most commonly used for VDSL2 Operation.

This section will not explain, in detail, the various Ethernet based options; as this must be specified by an ISPs Network Operations Center and OSP Manager.

**Step 1 Direct your browser to the WAN IF: Ethernet page**

**1.A** In the left-hand navigation pane, select:

**WAN**

**WAN IF: ETHERNET**

**Step 2 Create an Ethernet Interface**

**2.A Select “Add”**

**Notes:**
You must remove, and rebuild, an interface if you would like to change parameters.

Associated WAN Services must be removed, before an interface may be removed.

**2.B Select Ethernet Port**

**Notes:**

It is strongly suggested that the “Omni-Port” be used for WAN Operation.

The option to use another port if available, in the event that another

**2.C** Select “Apply / Save”

# SECTION 2.8  CREATE / MODIFY A BRIDGED WAN SERVICE

**Abstract**

This section will explain creating a Bridged WAN Service;  which removes any routing services from the WAN interface.

This section will not explain, in detail, the various options; as this must be specified by an ISP's Network Operations Center and OSP Manager.

**Step 1 Direct your browser to the WAN IF: Services page**

**1.A** In the left-hand navigation pane, select: **WAN**

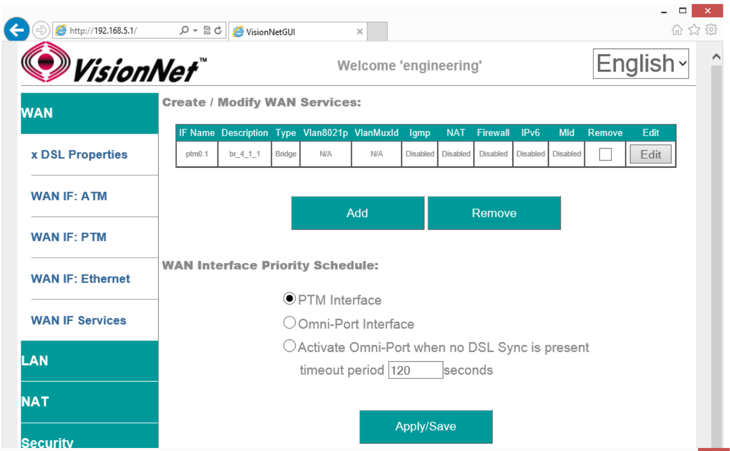
**WAN IF: Services**

**Step 2 Create a WAN Interface**

**2.A Select “Add”**

**Notes:**

NOTE: If you wish to modify an existing connection; select the “EDIT” button located in the table row of the desired interface



**Create / Modify WAN Services:**

| IF Name | Description | Type | Vlan8021p | VlanMuxId | Igmp | NAT | Firewall | IPv6 | Mld | Remove | Edit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ptm0.1 | br_4_1_1 | Bridge | N/A | N/A | Disabled | Disabled | Disabled | Disabled | Disabled | □ | Edit |

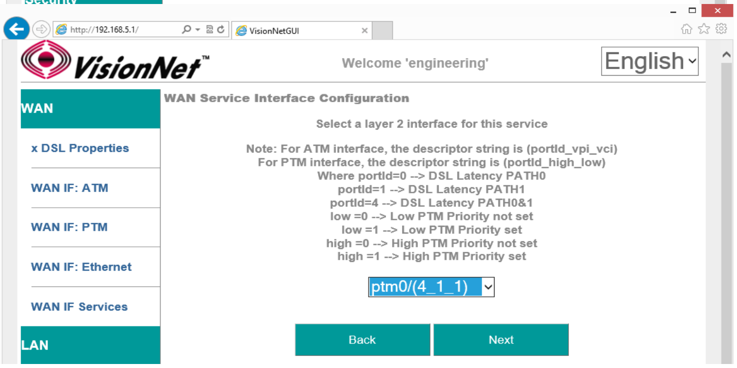
**WAN Interface Priority Schedule:**

● PTM Interface
○ Omni-Port Interface
○ Activate Omni-Port when no DSL Sync is present
timeout period 120 seconds

**2.B Select Desired Interface**

**This is the Interface that will be used for the Bridged Service**

**Upon selection, select “Next”**



**WAN Service Interface Configuration**

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

ptm0/(4_1_1)

## 2.C Specify Basic WAN Services

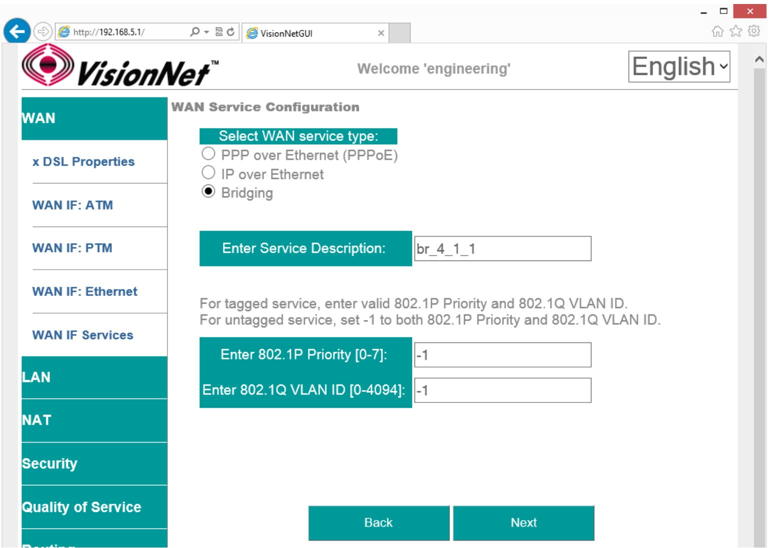
**WAN Service Type:** Bridging

**Service Description:** User Defined

**802.1p:** If untagged, leave as -1 (Null)

**802.1q:** If untagged, leave as -1 (Null)

Once complete, select "Next"



WAN Service Configuration

Select WAN service type:
○ PPP over Ethernet (PPPoE)
○ IP over Ethernet
● Bridging

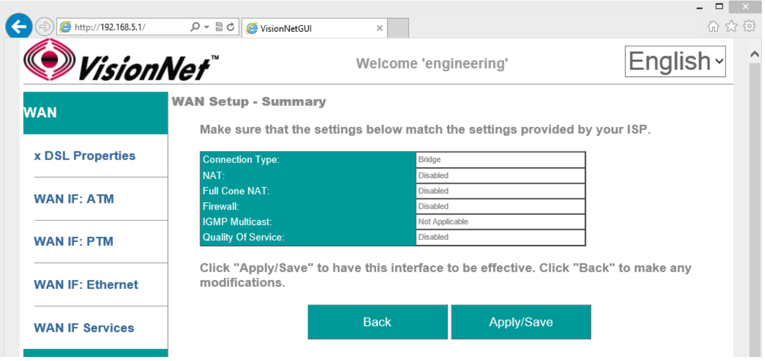
Enter Service Description: br_4_1_1

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]: -1
Enter 802.1Q VLAN ID [0-4094]: -1

## 2.D WAN Summary

Upon Review, select "Apply/Save"



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

| | |
|---|---|
| Connection Type: | Bridge |
| NAT: | Disabled |
| Full Cone NAT: | Disabled |
| Firewall: | Disabled |
| IGMP Multicast: | Not Applicable |
| Quality Of Service: | Disabled |

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

# SECTION 2.9 CREATE / MODIFY AN IPOE WAN SERVICE

**Abstract**

This section will explain creating an IPoE WAN Service;  which enables routing services.

This section will not explain, in detail, the various options; as this must be specified by an ISPs Network Operations Center and OSP Manager.

**Step 1 Direct your browser to the WAN IF: Services page**

**1.A** In the left-hand navigation pane, select:

WAN

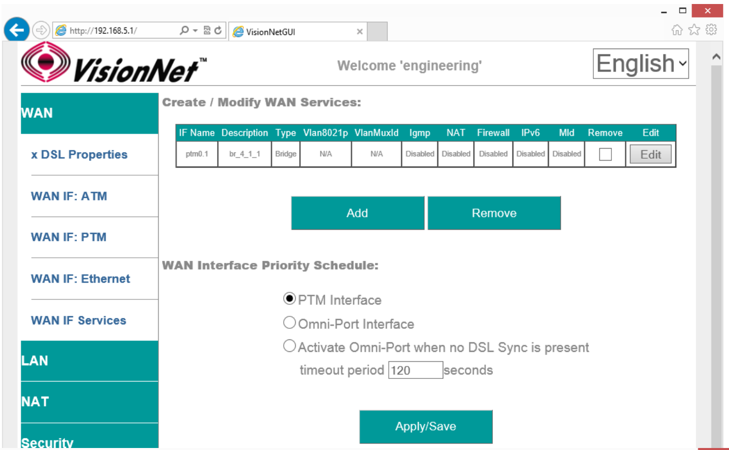
**WAN IF: Services**

**Step 2 Create a WAN Interface**

**2.A** **Select "Add"**

**Notes:**

NOTE: If you wish to modify an existing connection; select the "EDIT" button located in the table row of the desired interface



Welcome 'engineering'

Create / Modify WAN Services:

| IF Name | Description | Type | Vlan8021p | VlanMuxId | Igmp | NAT | Firewall | IPv6 | Mld | Remove | Edit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ptm0.1 | br_4_1_1 | Bridge | N/A | N/A | Disabled | Disabled | Disabled | Disabled | Disabled | □ | Edit |

Add  Remove

WAN Interface Priority Schedule:

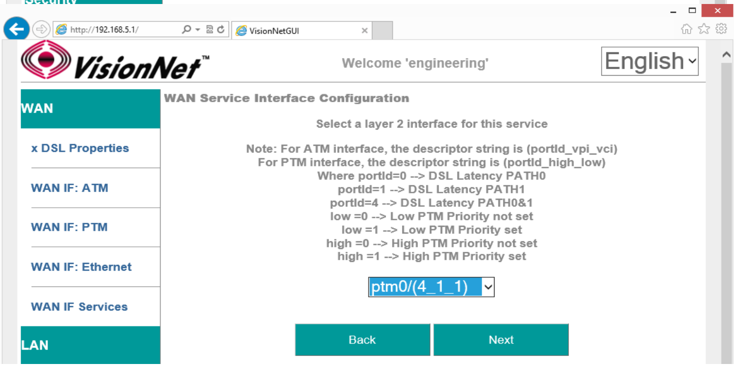
● PTM Interface
○ Omni-Port Interface
○ Activate Omni-Port when no DSL Sync is present
timeout period 120 seconds

Apply/Save

**2.B** **Select Desired Interface**

**This is the Interface that will be used for the Bridged Service**

**Upon selection, select "Next"**



Welcome 'engineering'

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

ptm0/(4_1_1)

Back  Next

## 2.C Specify Basic WAN Services

**WAN Service Type:** IPoE

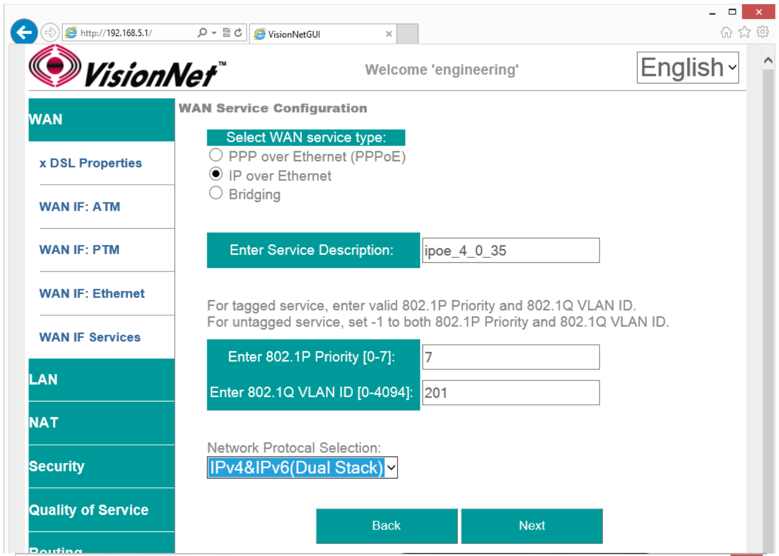
**Service Description:** User Defined

**802.1p:** If untagged, leave as -1 (Null)

**802.1q:** If untagged, leave as -1 (Null)

**Network Protocol:** IPv4, Dual Stack, or IPv6

Once complete, select "Next"



Welcome 'engineering'

WAN Service Configuration

Select WAN service type:
○ PPP over Ethernet (PPPoE)
● IP over Ethernet
○ Bridging

Enter Service Description: ipoe_4_0_35

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]: 7
Enter 802.1Q VLAN ID [0-4094]: 201

Network Protocal Selection:
IPv4&IPv6(Dual Stack)

## 2.D Specify WAN IP Settings

**WAN Service Type:** IPoE

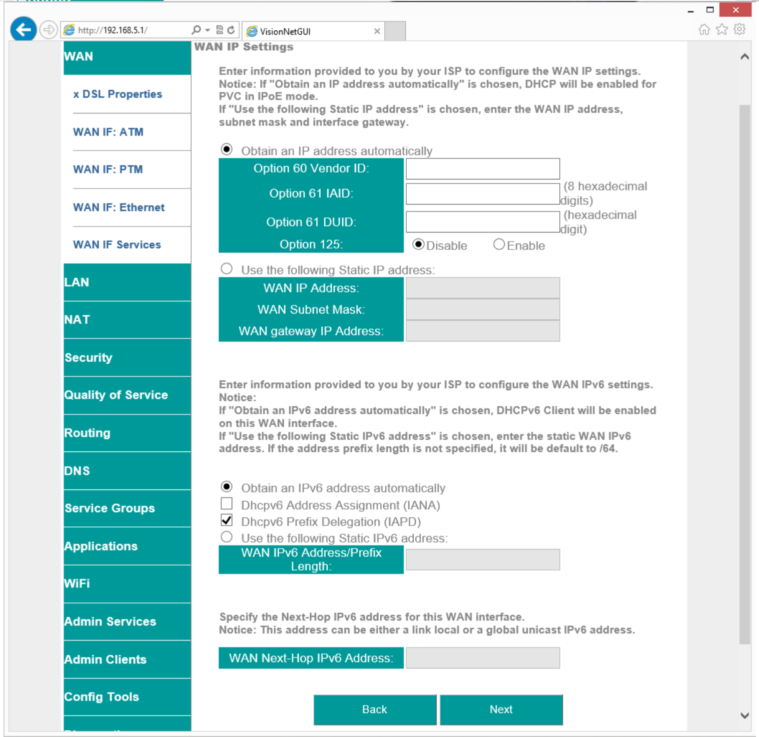
**IPv4**
Enable DHCP client plus desired additional DHCP Options

or enter Static IP Parameters

**IPv6:**
Specify applicable IPv6 Addresses

Static IPv6 may be applied; but is not advisable.

**Once complete, select "Next"**



WAN IP Settings

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.

● Obtain an IP address automatically
Option 60 Vendor ID:
Option 61 IAID: (8 hexadecimal digits)
Option 61 DUID: (hexadecimal digit)
Option 125: ● Disable ○ Enable

○ Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:

Enter information provided to you by your ISP to configure the WAN IPv6 settings.
Notice:
If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.
If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.

● Obtain an IPv6 address automatically
☐ Dhcpv6 Address Assignment (IANA)
☑ Dhcpv6 Prefix Delegation (IAPD)
○ Use the following Static IPv6 address:
WAN IPv6 Address/Prefix Length:

Specify the Next-Hop IPv6 address for this WAN interface.
Notice: This address can be either a link local or a global unicast IPv6 address.

WAN Next-Hop IPv6 Address:

## 2.E Specify WAN Services

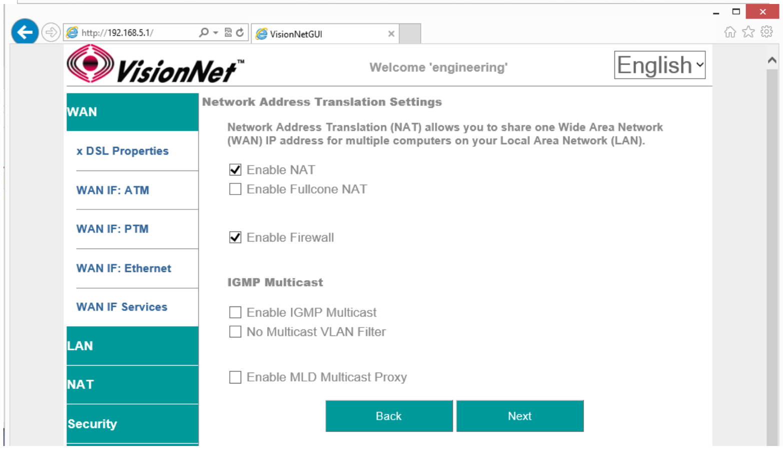
**NAT:**
Translation from WAN to LAN IPs

**Full Cone NAT:**
Augments NAT by keeping translated port associations open

**Firewall:**
Necessary for Management Services, Port Forwarding, etc.

**Enable IGMP Multicast:**
Only to be used, for IPTV WAN Services, where IGMP proxy is required. Do not enable otherwise.

**No Multicast VLAN Filter**



Welcome 'engineering'

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

☑ Enable NAT
☐ Enable Fullcone NAT

☑ Enable Firewall

IGMP Multicast

☐ Enable IGMP Multicast
☐ No Multicast VLAN Filter

☐ Enable MLD Multicast Proxy

Monitor all VLANs

**Enable MLD Multi-Cast Proxy**
Allows MLD outside of local domain

Once complete, select "Next"

## 2.F Add Service to Gateway Priority List

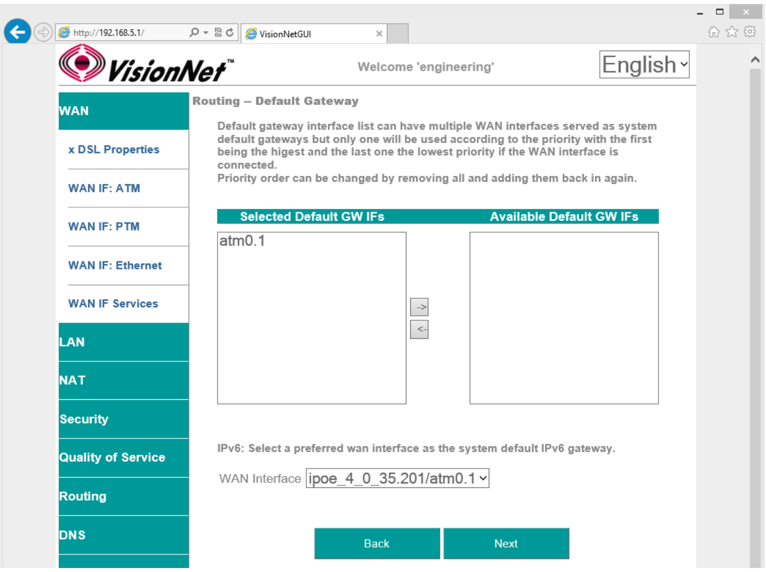
(Not available in WAN Modification; For post creation Modification See Section 4.1)

The Service will be available in the "Available Default GWs column".

Upon selection, you may place with the "Selected Default Gateways" column.

Gateway prioritization runs from top to bottom, and may be re-prioritized by removing WAN services from the left column; and then re-entering them in the desired order.

You may also select the IPv6 Default Gateway interface.



Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected.
Priority order can be changed by removing all and adding them back in again.

| Selected Default GW IFs | Available Default GW IFs |
|---|---|
| atm0.1 | |

IPv6: Select a preferred wan interface as the system default IPv6 gateway.

WAN Interface ipoe_4_0_35.201/atm0.1

## 2.G Add Service to DNS Priority List

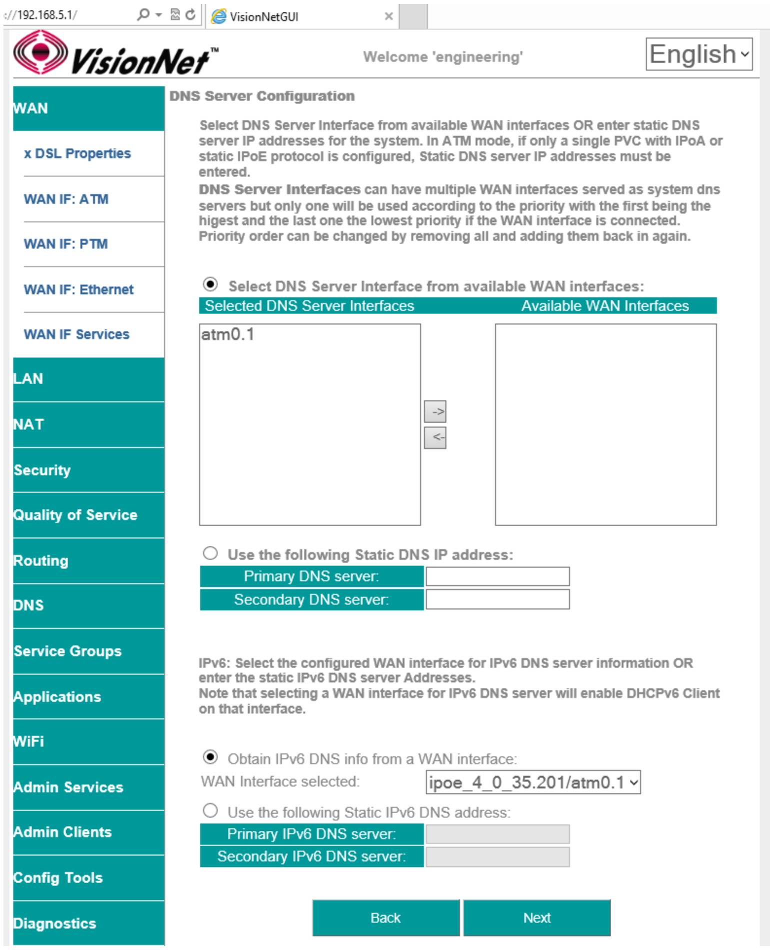
(Not available in WAN Modification; For post creation Modification See Section X)

The Service will be available in the "Available WAN Interfaces column".

Upon selection, you may place with the "Selected DNS Server Interfaces" column.

DNS Service Prioritization runs from top to bottom, and may be re-prioritized by removing WAN services from the left column; and then re-entering them in the desired order.

You may also select the IPv6 Default DNS Interface.



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected.
Priority order can be changed by removing all and adding them back in again.

● Select DNS Server Interface from available WAN interfaces:

| Selected DNS Server Interfaces | Available WAN Interfaces |
|---|---|
| atm0.1 | |

○ Use the following Static DNS IP address:

| | |
|---|---|
| Primary DNS server: | |
| Secondary DNS server: | |

IPv6: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

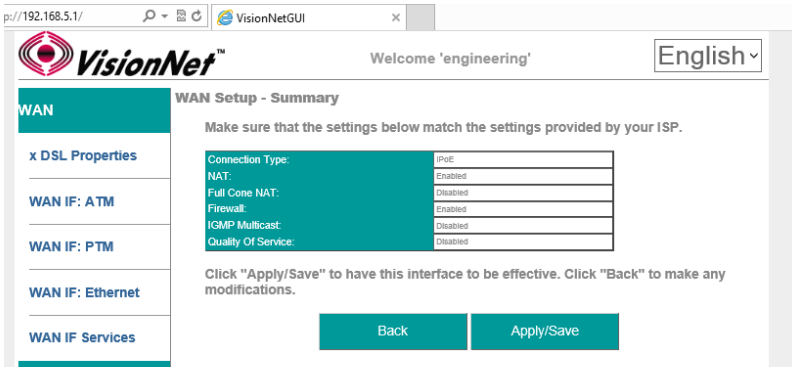
● Obtain IPv6 DNS info from a WAN interface:
WAN Interface selected: ipoe_4_0_35.201/atm0.1

○ Use the following Static IPv6 DNS address:

| | |
|---|---|
| Primary IPv6 DNS server: | |
| Secondary IPv6 DNS server: | |

## 2.H WAN Summary

**Upon Review, select “Apply/Save”**



Welcome 'engineering'

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

| | |
|---|---|
| Connection Type: | IPoE |
| NAT: | Enabled |
| Full Cone NAT: | Disabled |
| Firewall: | Enabled |
| IGMP Multicast: | Disabled |
| Quality Of Service: | Disabled |

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

# SECTION 2.10  CREATE / MODIFY A PPP WAN SERVICE

**Abstract**

This section will explain creating a PPP WAN Service, which may be used for routed, or proxied, IP services.

This section will not explain, in detail, the various options; as this must be specified by an ISPs Network Operations Center and OSP Manager.

**Step 1** **Direct your browser to the WAN IF: Services page**

**1.A** In the left-hand navigation pane, select:

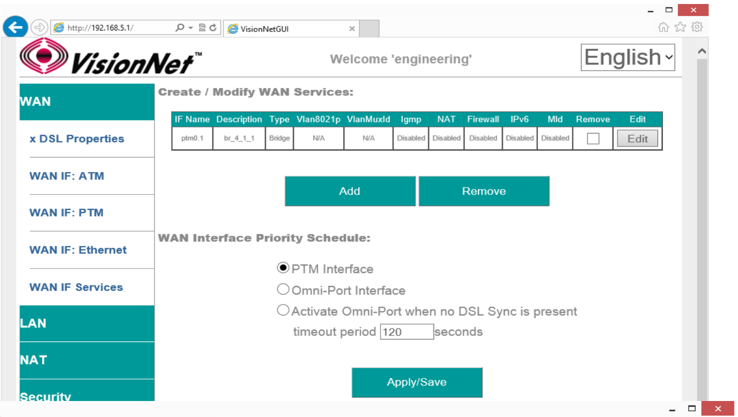
WAN

**WAN IF: Services**

**Step 2** **Create a WAN Interface**

**2.A** **Select "Add"**

NOTE: If you wish to modify an existing connection; select the "EDIT" button located in the table row of the desired interface



http://192.168.5.1/ VisionNetGUI

VisionNet™ Welcome 'engineering' English

WAN
x DSL Properties
WAN IF: ATM
WAN IF: PTM
WAN IF: Ethernet
WAN IF Services
LAN
NAT
Security

Create / Modify WAN Services:

| IF Name | Description | Type | Vlan8021p | VlanMuxId | Igmp | NAT | Firewall | IPv6 | Mld | Remove | Edit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ptm0.1 | br_4_1_1 | Bridge | N/A | N/A | Disabled | Disabled | Disabled | Disabled | Disabled | □ | Edit |

Add Remove

WAN Interface Priority Schedule:

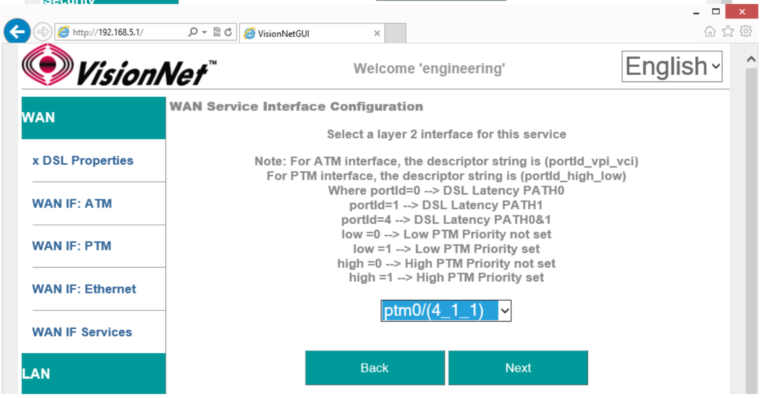
● PTM Interface
○ Omni-Port Interface
○ Activate Omni-Port when no DSL Sync is present
timeout period 120 seconds

Apply/Save

**2.B** **Select Desired Interface**

**This is the Interface that will be used for the Bridged Service**

**Upon selection, select "Next"**



http://192.168.5.1/ VisionNetGUI

VisionNet™ Welcome 'engineering' English

WAN
x DSL Properties
WAN IF: ATM
WAN IF: PTM
WAN IF: Ethernet
WAN IF Services
LAN

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

ptm0/(4_1_1)

Back Next

## 2.C Specify Basic WAN Services

**WAN Service Type:** PPPoE
*(PPPoA is only available if selected during ATM Creation; if this is the case, then there will be no option to select services)*

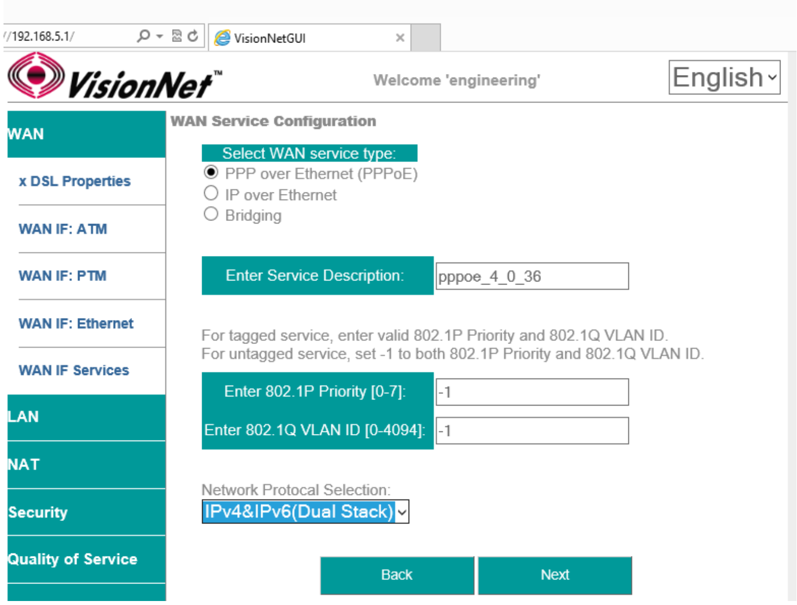
**Service Description:** User Defined

**802.1p:** If untagged, leave as -1 (Null)

**802.1q:** If untagged, leave as -1 (Null)

**Network Protocol:** IPv4, Dual Stack, or IPv6

Once complete, select "Next"



WAN Service Configuration

Select WAN service type:

● PPP over Ethernet (PPPoE)
○ IP over Ethernet
○ Bridging

Enter Service Description: pppoe_4_0_36

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

Network Protocal Selection:
IPv4&IPv6(Dual Stack)

## 2.D Specify WAN IP Settings

**PPP Authentication Client**
Username
Password
Service Name (usually blank)
Authentication Method (usually AUTO)

**NAT:**
Translation from WAN to LAN IPs

**Full Cone NAT:**
Augments NAT by keeping translated port associations open

**Firewall:**
Necessary for Management Services, Port Forwarding, etc.

**Dial on Demand:**
If enabled, PPP will disconnect, after the specified period of time, until hosts request internet access

**PPP IP Extension**
Disables NAT, and forward IP to first DHCP requesting host from LAN.

**Static IP Settings**
If Static IPs for v4, or v6, are to be assigned in lieu of DHCP

**IPv6 Settings**
IPv6 DHCP / RADVD settings

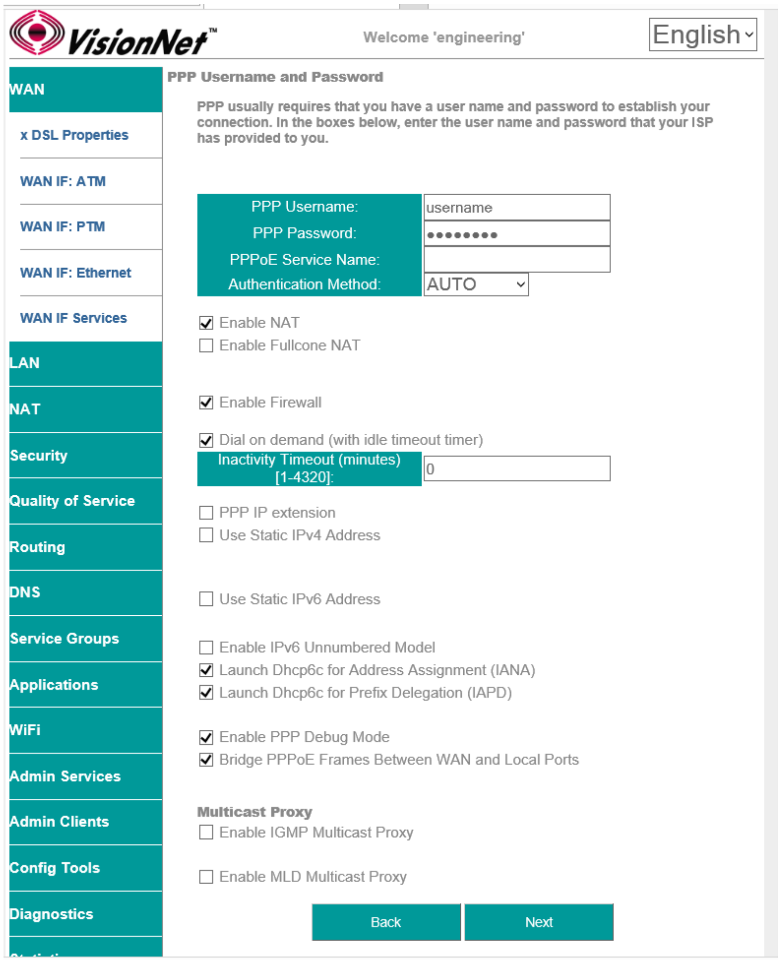
**PPP Debug Mode**
Sends all PPP service activity to syslog – for testing only

**Bridge PPPoE Frames between WAN and Local Ports**
Allows PPP Requests to be made from LAN Hosts

**Enable IGMP Multicast:**
Only to be used, for IPTV WAN Services, where IGMP proxy is required. Do not enable otherwise.

**Enable MLD Multi-Cast Proxy**
Allows MLD outside of local domain

Once complete, select “Next”



**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: | username |
| PPP Password: | •••••••• |
| PPPoE Service Name: | |
| Authentication Method: | AUTO |

☑ Enable NAT
☐ Enable Fullcone NAT

☑ Enable Firewall

☑ Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]: 0

☐ PPP IP extension
☐ Use Static IPv4 Address

☐ Use Static IPv6 Address

☐ Enable IPv6 Unnumbered Model
☑ Launch Dhcp6c for Address Assignment (IANA)
☑ Launch Dhcp6c for Prefix Delegation (IAPD)

☑ Enable PPP Debug Mode
☑ Bridge PPPoE Frames Between WAN and Local Ports

**Multicast Proxy**
☐ Enable IGMP Multicast Proxy

☐ Enable MLD Multicast Proxy

## 2.E Add Service to Gateway Priority List

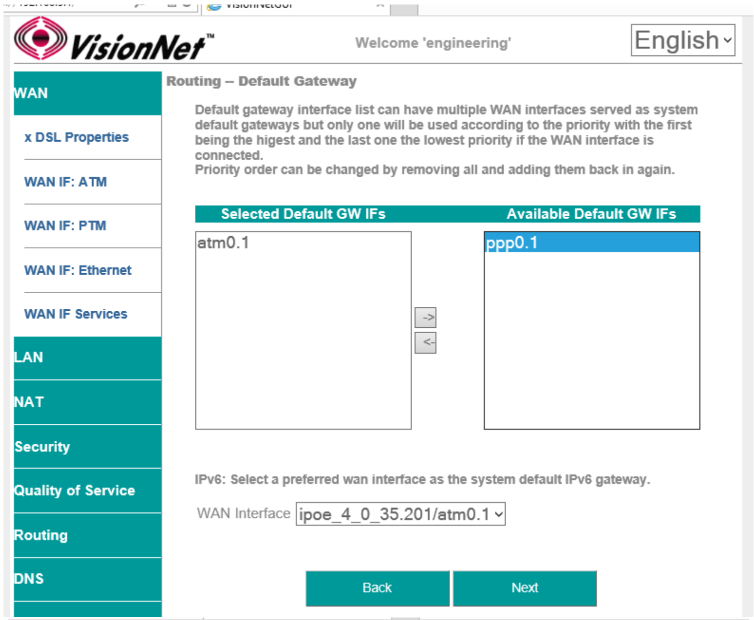
(Not available in WAN Modification; For post creation Modification See Section 4.1)

The Service will be available in the “Available Default GWs column”.

Upon selection, you may place with the “Selected Default Gateways” column.

Gateway prioritization runs from top to bottom, and may be re-prioritized by removing WAN services from the left column; and then re-entering them in the desired order.

You may also select the IPv6 Default Gateway interface.



Routing – Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected.
Priority order can be changed by removing all and adding them back in again.

| Selected Default GW IFs | Available Default GW IFs |
|---|---|
| atm0.1 | ppp0.1 |

IPv6: Select a preferred wan interface as the system default IPv6 gateway.

WAN Interface ipoe_4_0_35.201/atm0.1

## 2.F Add Service to DNS Priority List

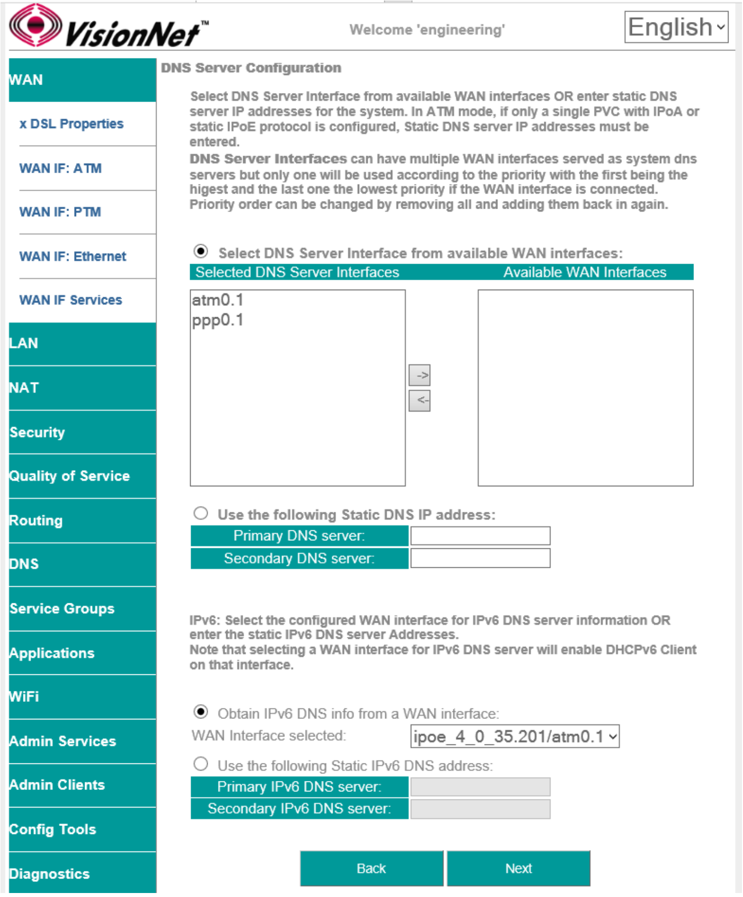
(Not available in WAN Modification; For post creation Modification See Section X)

The Service will be available in the “Available WAN Interfaces column”.

Upon selection, you may place with the “Selected DNS Server Interfaces” column.

DNS Service Prioritization runs from top to bottom, and may be re-prioritized by removing WAN services from the left column; and then re-entering them in the desired order.

You may also select the IPv6 Default DNS Interface.



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected.
Priority order can be changed by removing all and adding them back in again.

● Select DNS Server Interface from available WAN interfaces:

| Selected DNS Server Interfaces | Available WAN Interfaces |
|---|---|
| atm0.1<br>ppp0.1 | |

○ Use the following Static DNS IP address:

| | |
|---|---|
| Primary DNS server: | |
| Secondary DNS server: | |

IPv6: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

● Obtain IPv6 DNS info from a WAN interface:

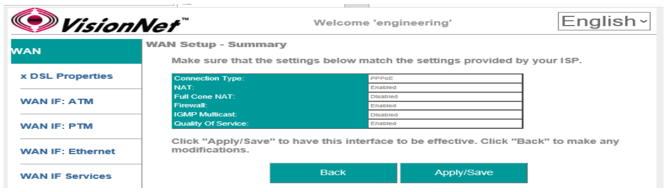
WAN Interface selected: ipoe_4_0_35.201/atm0.1

○ Use the following Static IPv6 DNS address:

| | |
|---|---|
| Primary IPv6 DNS server: | |
| Secondary IPv6 DNS server: | |

## 2.G WAN Summary

**Upon Review, select “Apply/Save”**



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

| | |
|---|---|
| Connection Type: | PPPoE |
| NAT: | Enabled |
| Full Cone NAT: | Disabled |
| Firewall: | Enabled |
| IGMP Multicast: | Disabled |
| Quality Of Service: | Enabled |

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

# SECTION 3: QUALITY OF SERVICE

## SECTION 3.1 QUALITY OF SERVICE ENABLE / DISABLE

**Abstract**

This section will depict enabling / disabling QoS for WAN Path Prioritization. QoS queues packets, based upon priority weight, for processor and transmittal priority.

**Step 1** **Direct your browser to the Enable QoS page**

1.A In the left-hand navigation pane, select:

**Quality of Service**

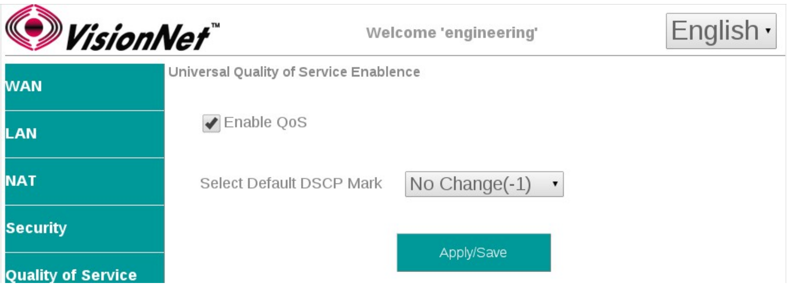
**Enable QoS**

**Step 2** **Enable / Disable QoS**

2.A **Enable QoS**
Default Disabled

**Default DSCP Mark**
Default No Change

Note: Default DSCP Mark will be used when creating Egress Class Rules



Universal Quality of Service Enablence

☑ Enable QoS

Select Default DSCP Mark: No Change(-1)

2.B When finished, select " Apply / Save ".

## SECTION 3.2 Interface Configuration

### Abstract

This section will depict enabling / disabling QoS rules for specific WAN Interfaces

**Step 1 Direct your browser to the QoS Queue page**

**1.A** In the left-hand navigation pane, select:

**Quality of Service**

**QoS Queue**

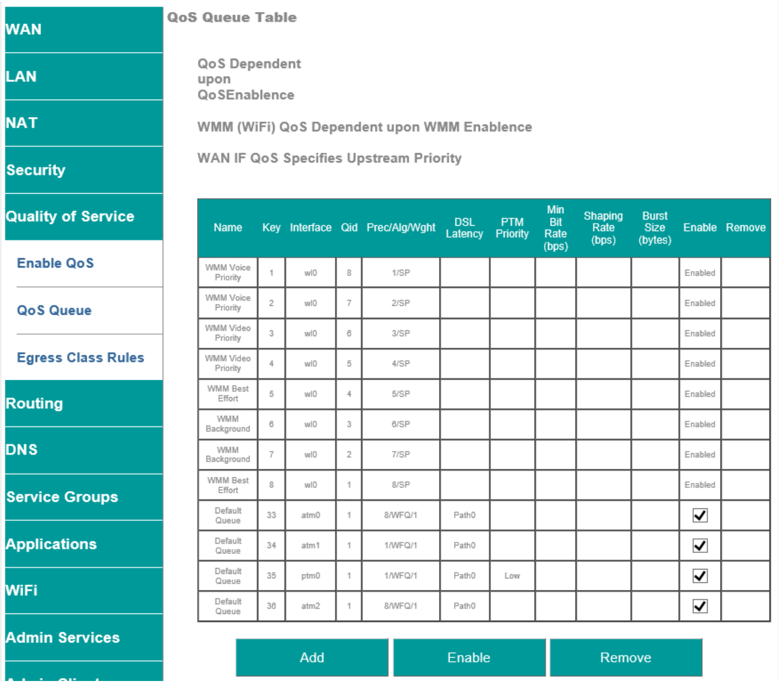
**Step 2 Enable / Disable Interfaces**

**2.A** **WMM Priorities**
These apply to WiFi, when WMM is enabled

**Enable / Disable WAN Interfaces**
Check / Uncheck the radio box within the table row of the desired interface.

**Adding Interface**
You may add interfaces, to this list, by selecting add.

**Note: The add feature applies primarily to Ethernet port prioritization.**



QoS Queue Table

QoS Dependent upon QoSEnablence

WMM (WiFi) QoS Dependent upon WMM Enablence

WAN IF QoS Specifies Upstream Priority

| Name | Key | Interface | Qid | Prec/Alg/Wght | DSL Latency | PTM Priority | Min Bit Rate (bps) | Shaping Rate (bps) | Burst Size (bytes) | Enable | Remove |
|---|---|---|---|---|---|---|---|---|---|---|---|
| WMM Voice Priority | 1 | wl0 | 8 | 1/SP | | | | | | Enabled | |
| WMM Voice Priority | 2 | wl0 | 7 | 2/SP | | | | | | Enabled | |
| WMM Video Priority | 3 | wl0 | 6 | 3/SP | | | | | | Enabled | |
| WMM Video Priority | 4 | wl0 | 5 | 4/SP | | | | | | Enabled | |
| WMM Best Effort | 5 | wl0 | 4 | 5/SP | | | | | | Enabled | |
| WMM Background | 6 | wl0 | 3 | 6/SP | | | | | | Enabled | |
| WMM Background | 7 | wl0 | 2 | 7/SP | | | | | | Enabled | |
| WMM Best Effort | 8 | wl0 | 1 | 8/SP | | | | | | Enabled | |
| Default Queue | 33 | atm0 | 1 | 8/WFQ/1 | Path0 | | | | | ☑ | |
| Default Queue | 34 | atm1 | 1 | 1/WFQ/1 | Path0 | | | | | ☑ | |
| Default Queue | 35 | ptm0 | 1 | 1/WFQ/1 | Path0 | Low | | | | ☑ | |
| Default Queue | 36 | atm2 | 1 | 8/WFQ/1 | Path0 | | | | | ☑ | |

**2.B** When finished, select " Apply / Save ".

# SECTION 3.3 QoS Classification Table

## Abstract

This section will depict the QoS Classification Table

**Step 1** **Direct your browser to the Egress Class Rules page**

**1.A** In the left-hand navigation pane, select:

**Quality of Service**

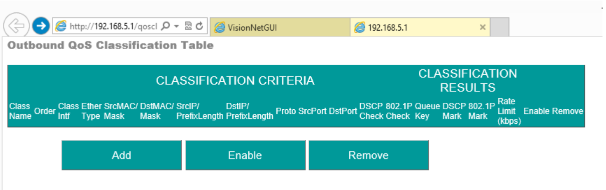
**Egress Class Rules**

**Step 2** **Add Entry**

**2.A** **Note: Your browser will open the table in a new tab.**

This is due to browser size limitations

Upon Review, select “Add”



http://192.168.5.1/qoscl — VisionNetGUI — 192.168.5.1

**Outbound QoS Classification Table**

| CLASSIFICATION CRITERIA | | | | | | | | | | | | | CLASSIFICATION RESULTS | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Class Name | Order | Class Intf | Ether Type | SrcMAC/ Mask | DstMAC/ Mask | SrcIP/ PrefixLength | DstIP/ PrefixLength | Proto | SrcPort | DstPort | DSCP Check | 802.1P Check | Queue Key | DSCP Mark | 802.1P Mark | Rate Limit (kbps) | Enable | Remove |

**Step 3** **Customize Rule**

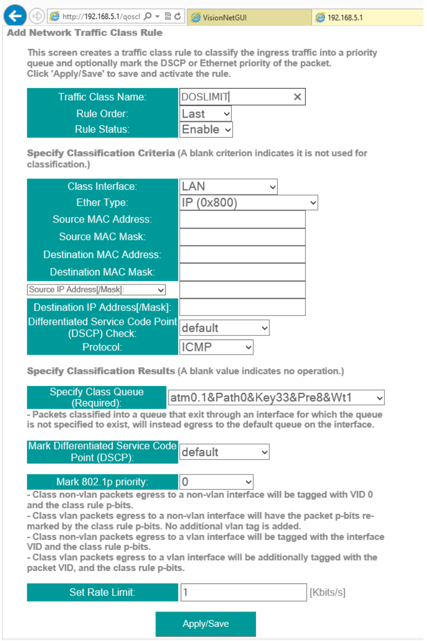
**3.A** General Guidelines

The first section is to establish the Rule Identifier and Status

The second section is to establish which type of packets will be considered for QoS

The third section is to establish the patch, DSCP, Priority, and any egress rate limiting

When complete, select “Apply / Save”



http://192.168.5.1/qoscl — VisionNetGUI — 192.168.5.1

**Add Network Traffic Class Rule**

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet.
Click 'Apply/Save' to save and activate the rule.

| | |
|---|---|
| Traffic Class Name: | DOSLIMIT |
| Rule Order: | Last |
| Rule Status: | Enable |

**Specify Classification Criteria** (A blank criterion indicates it is not used for classification.)

| | |
|---|---|
| Class Interface: | LAN |
| Ether Type: | IP (0x800) |
| Source MAC Address: | |
| Source MAC Mask: | |
| Destination MAC Address: | |
| Destination MAC Mask: | |
| Source IP Address[/Mask]: | |
| Destination IP Address[/Mask]: | |
| Differentiated Service Code Point (DSCP) Check: | default |
| Protocol: | ICMP |

**Specify Classification Results** (A blank value indicates no operation.)

| | |
|---|---|
| Specify Class Queue (Required): | atm0.1&Path0&Key33&Pre8&Wt1 |

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

| | |
|---|---|
| Mark Differentiated Service Code Point (DSCP): | default |
| Mark 802.1p priority: | 0 |

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

| | |
|---|---|
| Set Rate Limit: | 1 [Kbits/s] |

**3.B** When finished, select “ Apply / Save “.

# SECTION 4: SERVICE GROUPS

## SECTION 4.1 Service Group Logic

### Item 1 Service Group Abstract

Service Grouping, sometimes referred to as Port Mapping or VLAN Mapping, is a method of isolating WAN Services to individual broadcast / multicast domains.

### Item 2 Service Group Operation

**2.A WAN Services are grouped by service type.**

It is common, when multiple WAN Types are used for fallback or redundancy, that WAN Services of the same purpose are grouped together. IE:

Internet Service Group
ADSL2+ ATM 0.35
VDS2 PTM – VLAN 100

IPTV Service Group
ADSL2+ ATM 0.36
VDS2 PTM – VLAN 20

MGMT Service Group
ADSL2+ ATM 0.33
VDS2 PTM – VLAN 10

**2.B LAN Interfaces are then grouped by service type. IE:**

Internet Service Group
192.168.6.1/24
Ethernet 3
WiFi SSID

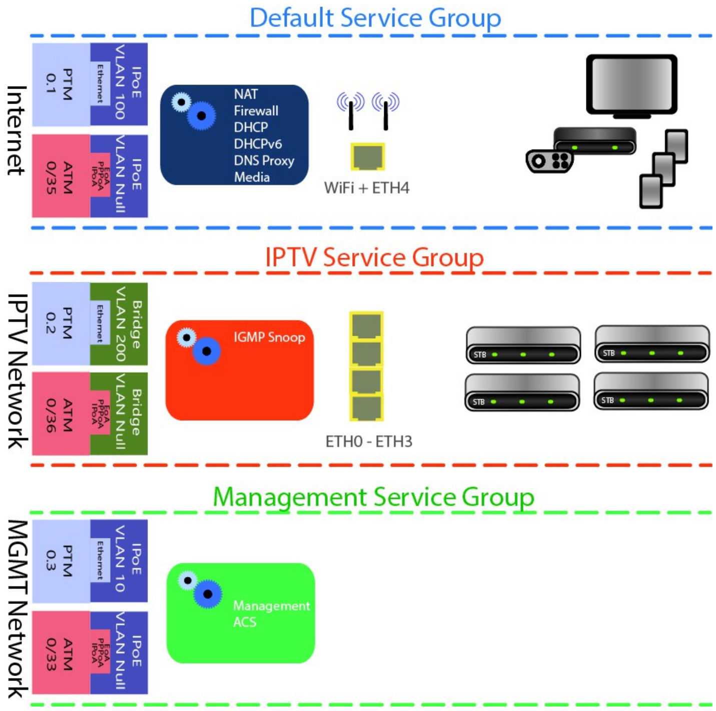
IPTV Service Group
192.168.2.1/24
Ethernet – 0 to 3

MGMT Service Group
192.168.4.1/24
Gateway MGMT Services

**2.C LAN Services are then specified for each Domain. IE:**

Internet Service Group
DHCP, DNS, Multicast/MLD Snoop

IPTV Service Group
Multicast / MLD Snoop



# SECTION 4.2 SERVICE GROUP CREATION

**Abstract**

This section will depict the creation of a Service Group, and will end with a list of items to be further defined post-creation.

The management device should be connected to a port that will ultimately be assigned to the 'default' service group.

**Step 1** **Direct your browser to the IF / Service Groups page**

**1.A** In the left-hand navigation pane, select:

Service Groups

IF / Service Groups

**Step 2** **Create a Service Group**

**2.A** **Group Name**

This is the name for your Service Group

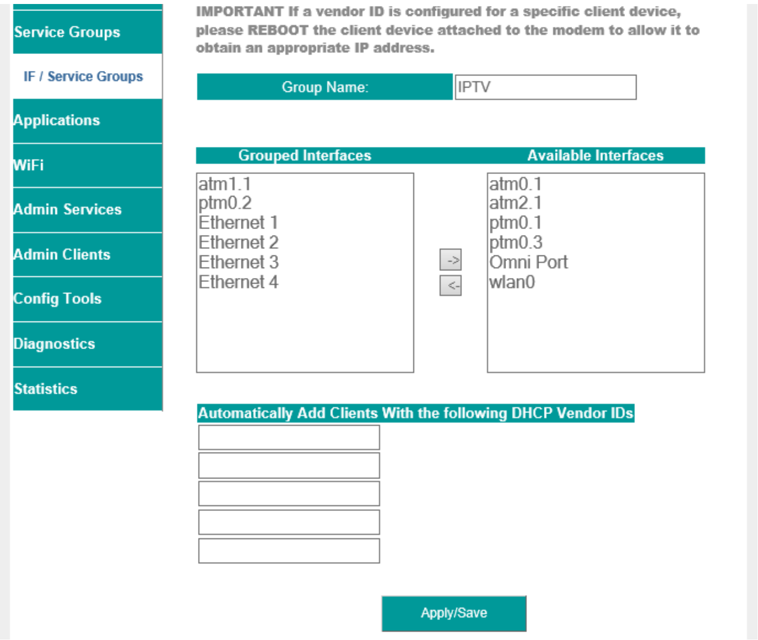
**Grouped Interfaces**

Interfaces may be taken, from the default group, and placed within the desired interface.

WAN Services and LAN Interfaces, within the same Service Group, will operate as one domain.

**DHCP Vendor IDs**

This is the BootP, Option 60, ID



**IMPORTANT** If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name: IPTV

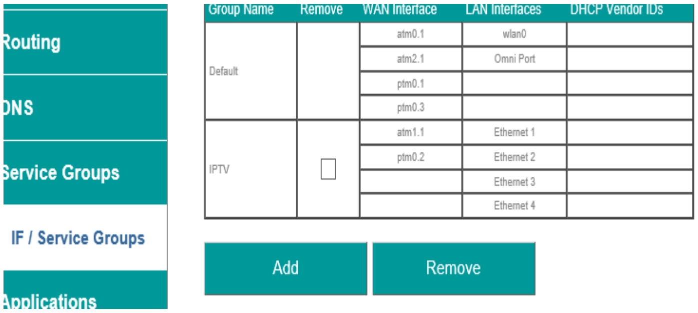
| Grouped Interfaces | Available Interfaces |
|---|---|
| atm1.1<br>ptm0.2<br>Ethernet 1<br>Ethernet 2<br>Ethernet 3<br>Ethernet 4 | atm0.1<br>atm2.1<br>ptm0.1<br>ptm0.3<br>Omni Port<br>wlan0 |

Automatically Add Clients With the following DHCP Vendor IDs

**Step 3** **When finished, select " Apply / Save ".**

The WAN and Ethernet Interfaces will now be listed as a separate group.

The LAN and Routing must be specified for each service group.



| Group Name | Remove | WAN Interface | LAN Interfaces | DHCP Vendor IDs |
|---|---|---|---|---|
| Default | | atm0.1 | wlan0 | |
| | | atm2.1 | Omni Port | |
| | | ptm0.1 | | |
| | | ptm0.3 | | |
| IPTV | □ | atm1.1 | Ethernet 1 | |
| | | ptm0.2 | Ethernet 2 | |
| | | | Ethernet 3 | |
| | | | Ethernet 4 | |

**Provisioning of service groups is not complete** until you have configured the LAN Services, This will be detailed in the next section

# SECTION 5: IPv4 LAN CONFIGURATION

## SECTION 5.1 IPv4 Configuration

**Abstract**

This section will depict the configuration of LAN broadcast groups. Each service group has separate IP, broadcast, and multi-cast domains. **You must configure LAN Services for each service group**

**Step 1** **Direct your browser to the LAN IPv4 page**

**1.A** In the left-hand navigation pane, select: **LAN**

**IPv4**

**Step 2** **Configure Service Group LAN Parameters**

**2.A** **Service Group**

Select Service Group to Modify

**LAN Firewall**

When enabled, hosts will not be able to manage device via Service Group LAN IP.

**Enable IGMP Snooping**

When enabled, the IGMP Multicast controller will be enabled.
Standard Mode will enable snooping
Blocking Mode will prevent Multicasts

**LAN IP Configuration**

Gateway IP / Subnet
This will serve as the LAN Gateway IP for hosts.

**DHCP Server**

Configure DHCP Range within Gateway Subnet

Enter Gateway IP, for DNS Servers, if proxy is to be used.

Enter custom DNS Servers if desired.

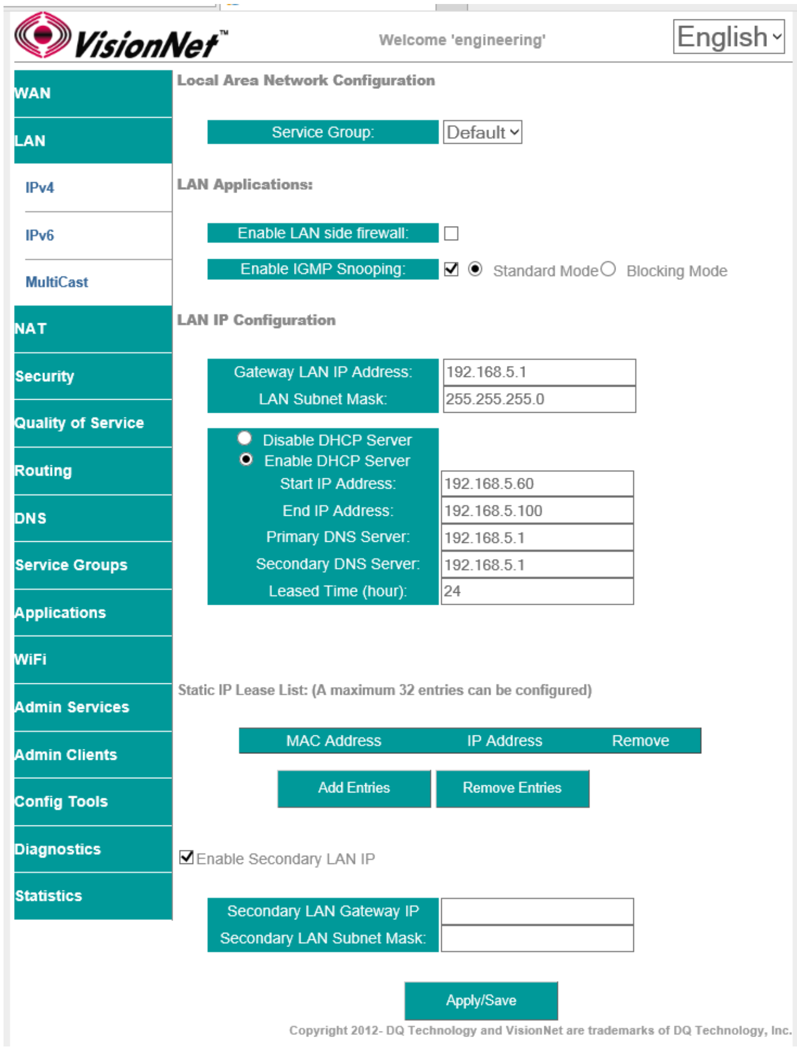
DNS Proxy may be by-passed (WAN DNS will be passed to devices). See Section 4.X

**DHCP Reservation (Static IP Lease)**

Reserve IPs, within the Primary Gateway Subnet, based upon hosts MAC Addresses

**Enable Secondary LAN IP**

A secondary LAN IP may be implemented. No DHCP Services are assigned to this interface



Local Area Network Configuration

Service Group: Default

LAN Applications:

Enable LAN side firewall: □

Enable IGMP Snooping: ☑ ● Standard Mode ○ Blocking Mode

LAN IP Configuration

| | |
|---|---|
| Gateway LAN IP Address: | 192.168.5.1 |
| LAN Subnet Mask: | 255.255.255.0 |

○ Disable DHCP Server
● Enable DHCP Server

| | |
|---|---|
| Start IP Address: | 192.168.5.60 |
| End IP Address: | 192.168.5.100 |
| Primary DNS Server: | 192.168.5.1 |
| Secondary DNS Server: | 192.168.5.1 |
| Leased Time (hour): | 24 |

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

| MAC Address | IP Address | Remove |
|---|---|---|

☑ Enable Secondary LAN IP

| | |
|---|---|
| Secondary LAN Gateway IP | |
| Secondary LAN Subnet Mask: | |

Copyright 2012- DQ Technology and VisionNet are trademarks of DQ Technology, Inc.

**Step 3** **When finished, select " Apply / Save ".**

# SECTION 5.2 IGMP MULTICAST

**Abstract**

**IGMP MultiCasting controls IPv4 snooping. IPv6 utilizes Multi-Casting in lieu of Broadcasting; and will be discussed later in this guide.**

**Step 1 Direct your browser to the LAN MultiCast page**

**1.A** In the left-hand navigation pane, select:

**LAN**

**MultiCast**

**Step 2 Configure IGMP Multi-Cast Parameters**

**2.A Multicast Precedence:**

Global precedence over unicast.

DO NOT ENABLE THIS FEATURE UNLESS REQUIRED FOR YOUR NETWORK. PIXELATION OF IPTV CAN OCCUR IF THIS IS ENABLED WITHOUT THE APPROPRIATE NETWORK ARCHITECTURE.

**IGMP Default Version:**

Default Version 3.
Version 3 backwards compatible to 2; but may not be supported upstream if IGMP 2 is used for the WAN Side network

**Query Interval**Default 125

**Query Response Interval** Default 10

**Last Member Query Interval** Default 10

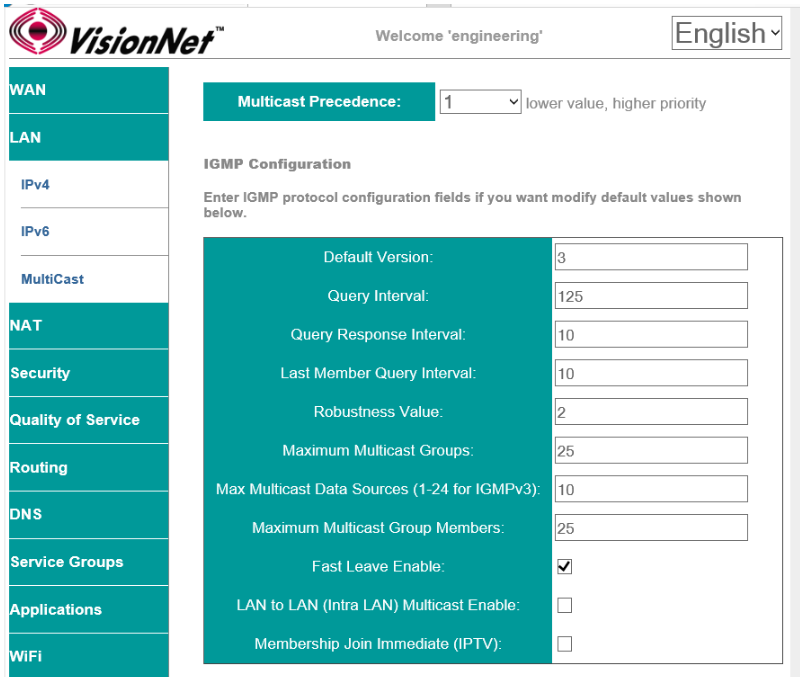
**Robustness Value** Default 2

**Max Multicast Group Members:** 25

**Fast Leave Enabled:** Default Enabled

**Intra LAN Multicast:** Default Disabled

**Membership Join Immediate: Default Disabled**



Multicast Precedence: 1 lower value, higher priority

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

| | |
|---|---|
| Default Version: | 3 |
| Query Interval: | 125 |
| Query Response Interval: | 10 |
| Last Member Query Interval: | 10 |
| Robustness Value: | 2 |
| Maximum Multicast Groups: | 25 |
| Max Multicast Data Sources (1-24 for IGMPv3): | 10 |
| Maximum Multicast Group Members: | 25 |
| Fast Leave Enable: | ☑ |
| LAN to LAN (Intra LAN) Multicast Enable: | ☐ |
| Membership Join Immediate (IPTV): | ☐ |

**Step 3 When finished, select " Apply / Save ".**

# SECTION 6: IPv4 ROUTE CONFIGURATION

## SECTION 6.1 GATEWAY PRIORITIZATION

**Abstract**

**Once routed WAN Services have been created, they may be globally prioritized.**

**Step 1** **Direct your browser to the IF Default Gateway page**

**1.A** In the left-hand navigation pane, select: **Routing**

**IF Default Gateway**

**Step 2** **Prioritize Default Gateway Information**

**2.A** **Add Service to Gateway Priority List**

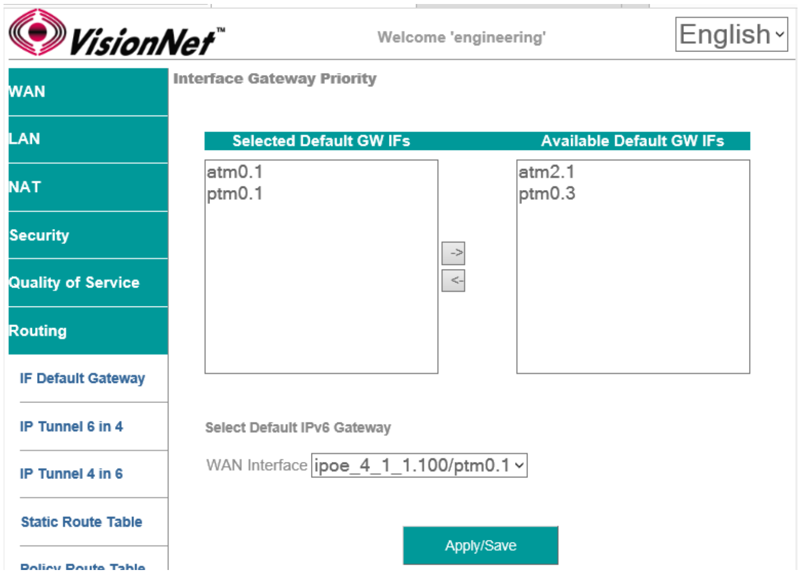
Available Interfaces will be available in the column labeled “Available Default GWs IFs”.

Select the WAN IFs, to be utilized as outbound paths, and move them to the column labeled “Selected Default GW IFs”.

Gateways are prioritized from the top down. In order to change the prioritization order, you must remove the interfaces and place them in the desired order.

NOTE: Option 121 does not need to be assigned to the primary Gateway; but rather the gateway that is the primary outbound path for advertised routes.

Only one WAN Service can receive option 121 route paths.



Interface Gateway Priority

| Selected Default GW IFs | Available Default GW IFs |
|---|---|
| atm0.1<br>ptm0.1 | atm2.1<br>ptm0.3 |

Select Default IPv6 Gateway

WAN Interface ipoe_4_1_1.100/ptm0.1

**Step 3** **When finished, select “ Apply / Save “.**

# SECTION 6.2 STATIC ROUTE TABLE

**Abstract**

**Once routed WAN Services have been created, outbound paths may be statically assigned.**

**The Static Route Table is defined by the Destination.**

**Step 1 Direct your browser to the Static Route Table page**

**1.A** In the left-hand navigation pane, select:

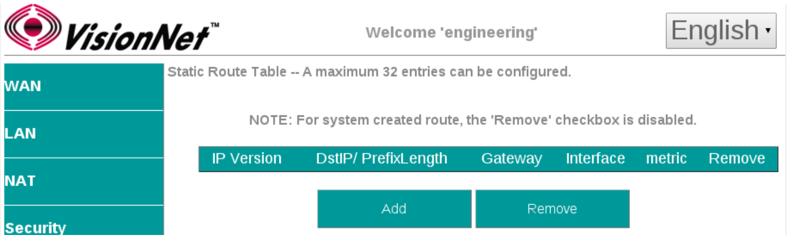
**Routing**

**Static Route Table**

**Step 2 Create the Static Route Table**

**2.A Add entry to Route Table**

Select **"Add"**



Static Route Table -- A maximum 32 entries can be configured.

NOTE: For system created route, the 'Remove' checkbox is disabled.

| IP Version | DstIP/ PrefixLength | Gateway | Interface | metric | Remove |
|---|---|---|---|---|---|

**2.B Create the Table Entry**

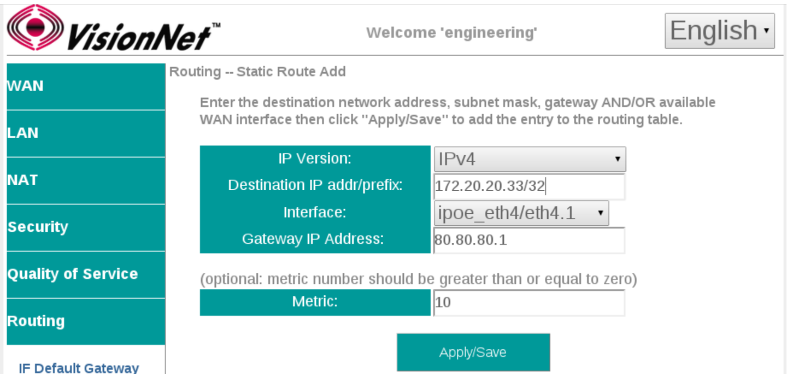
**IP Version:** v4 or v6

**Destination IP / Prefix:**
This must be entered in a standard format.
IPv6 Address compression is not supported.

**Interface:**
Select WAN Service for Outbound Path

**Gateway IP Address:**
This is the first outbound hop addresses

**Metric:**
This is the number of "hops" in the TTL



Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

| | |
|---|---|
| IP Version: | IPv4 |
| Destination IP addr/prefix: | 172.20.20.33/32 |
| Interface: | ipoe_eth4/eth4.1 |
| Gateway IP Address: | 80.80.80.1 |

(optional: metric number should be greater than or equal to zero)

| | |
|---|---|
| Metric: | 10 |

**Step 3 When finished, select " Apply / Save ".**

# SECTION 6.3 POLICY ROUTE TABLE

**Abstract**

**Once routed WAN Services have been created, outbound paths may be statically assigned**

**The Policy Route is defined by the originating Source.**

**Step 1** **Direct your browser to the Static Route Table page**

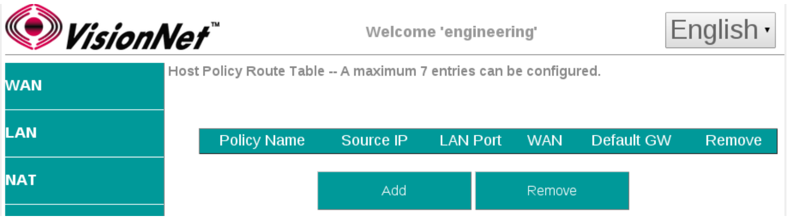
**1.A** In the left-hand navigation pane, select: **Routing**

**Policy Route Table**

**Step 2** **Prioritize Default Gateway Information**

**2.A** **Add Entry to Route Table**

Select **"Add"**



Host Policy Route Table -- A maximum 7 entries can be configured.

| Policy Name | Source IP | LAN Port | WAN | Default GW | Remove |
|---|---|---|---|---|---|

**2.B** **Create the Table Entry**

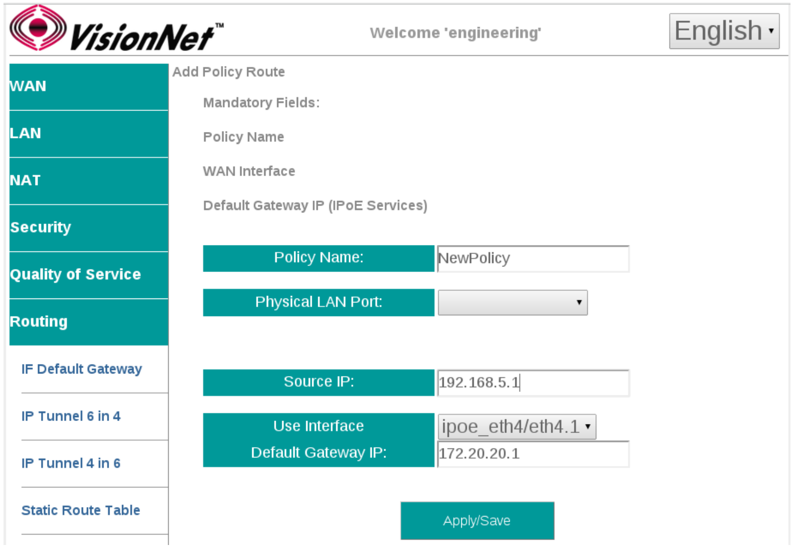
**Policy Name: User Defined**

**Physical LAN Port**
This can be left un-specified if you wish to use the Source IP only.

Source IP:
This is the LAN IP of the host - this can be left blank of a Physical LAN Port is to be specified.

**Use Interface**
This specifies the Outbound WAN IF

**Gateway IP Address:**
This is the first outbound hop addresses



Add Policy Route

Mandatory Fields:

Policy Name

WAN Interface

Default Gateway IP (IPoE Services)

Policy Name: NewPolicy

Physical LAN Port:

Source IP: 192.168.5.1

Use Interface: ipoe_eth4/eth4.1

Default Gateway IP: 172.20.20.1

**Step 3** **When finished, select " Apply / Save ".**

# SECTION 7: IPv4 DNS CONFIGURATION

## SECTION 7.1 GLOBAL DNS PRIORITIZATION

**Abstract**

**Once routed WAN services have been created, you may prioritize the dynamically assigned DNS servers that the CPE utilizes for DNS resolution.**

**Step 1 Direct your browser to the IF Default DNS page**

**1.A** In the left-hand navigation pane, select:

**DNS**

**IF Default DNS**

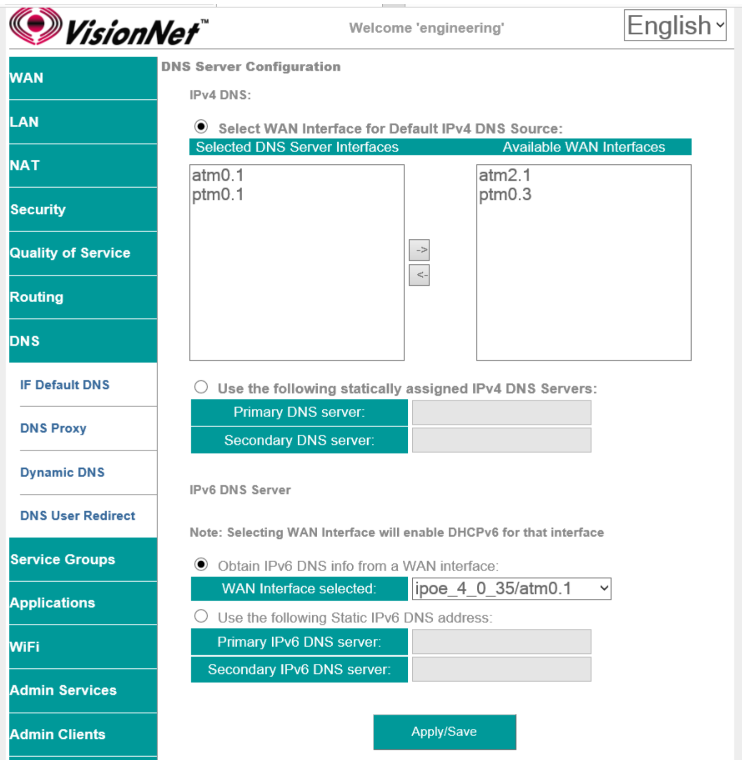
**Step 2 Prioritize DNS Server Paths**

**2.A Select IFs for DNS Resolution**

Available Interfaces will be available in the column labeled “Available WAN IFs”.

Select the WAN IFs, to be utilized for DNS Resolution, and move them to the column labeled “Selected DNS Server Interfaces”.

WAN DNS Interfaces are prioritized from the top down. In order to change the prioritization order, you must remove the interfaces and place them in the desired order.



DNS Server Configuration

IPv4 DNS:

● Select WAN Interface for Default IPv4 DNS Source:

| Selected DNS Server Interfaces | Available WAN Interfaces |
|---|---|
| atm0.1<br>ptm0.1 | atm2.1<br>ptm0.3 |

○ Use the following statically assigned IPv4 DNS Servers:

Primary DNS server:

Secondary DNS server:

IPv6 DNS Server

Note: Selecting WAN Interface will enable DHCPv6 for that interface

● Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected: ipoe_4_0_35/atm0.1

○ Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

**Step 3 When finished, select “ Apply / Save “.**

# SECTION 7.2 STATICALLY ASSIGNED GLOBAL DNS

**Abstract**

**You may over-ride the dynamically assigned DNS settings, to manually assign the DNS Servers that the gateway CPE uses for name resolution.**

**Step 1** **Direct your browser to the IF Default DNS page**

**1.A** In the left-hand navigation pane, select: **DNS**

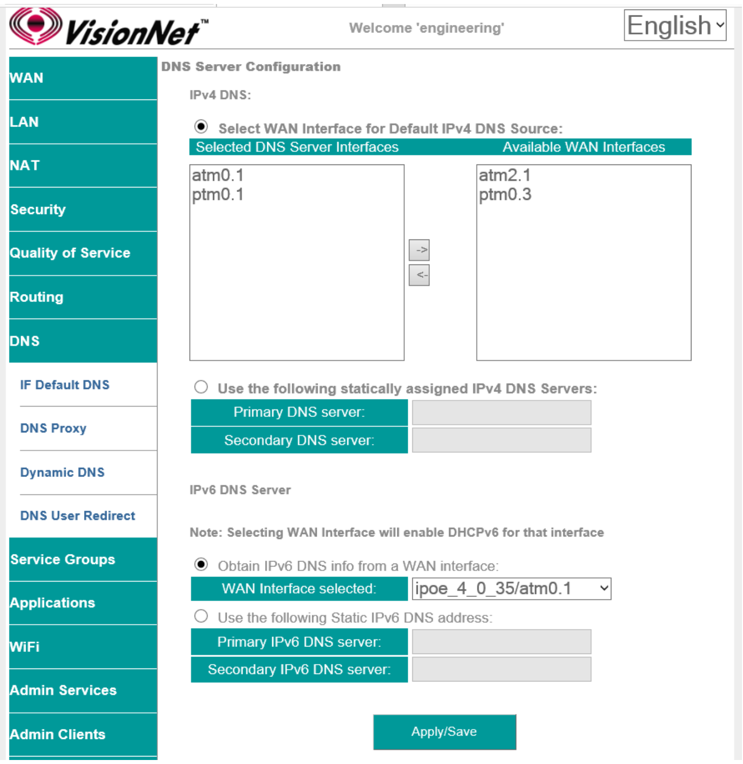
**IF Default DNS**

**Step 2** **Statically Assign DNS Servers**

**2.A** **Select IFs "Use the following statically assinged IPv4 DNS Servers".**

**IPv4**

Enter Primary and Secondary



DNS Server Configuration

IPv4 DNS:

● Select WAN Interface for Default IPv4 DNS Source:

| Selected DNS Server Interfaces | Available WAN Interfaces |
|---|---|
| atm0.1<br>ptm0.1 | atm2.1<br>ptm0.3 |

○ Use the following statically assigned IPv4 DNS Servers:

| | |
|---|---|
| Primary DNS server: | |
| Secondary DNS server: | |

IPv6 DNS Server

Note: Selecting WAN Interface will enable DHCPv6 for that interface

● Obtain IPv6 DNS info from a WAN interface:

| | |
|---|---|
| WAN Interface selected: | ipoe_4_0_35/atm0.1 |

○ Use the following Static IPv6 DNS address:

| | |
|---|---|
| Primary IPv6 DNS server: | |
| Secondary IPv6 DNS server: | |

**Step 3** **When finished, select " Apply / Save ".**

# SECTION 8: IPv4 NAT TRAVERSAL

## SECTION 8.1 UPnP

**Abstract**

**Once a Routed IPv4 WAN Interface has been created, and NAT Assigned, there may be a need to alter the way that specific applications traverse NAT.**

**UPnP dynamically opens and forwards  specific ports, requested by host applications, to be exposed to the internet.**

**UPnP is most commonly associated with gaming systems, Internet enabled surveilance systems, and AntiVirus Teredo Tunnels.**

**While UPnP is used by many devices, it is also a potential security risk. UPnP allows devices to act as public servers, with no human configuration; and should used only when necessary.**

**Step 1** **Direct your browser to the UPnP page**

**1.A** In the left-hand navigation pane, select:

**NAT**

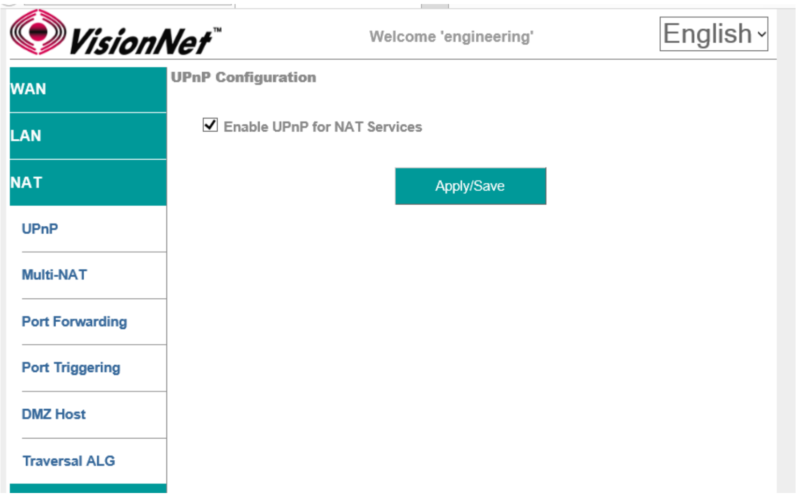
**UPnP**

**Step 2** **Enable / Disable UPnP**

**2.A** **UPnP, when enabled, will utilize the ports requested by hosts.**

**This could cause the default ports, used for management, to change.**

**For this reason, non-standard management ports are always suggested.**



Welcome 'engineering'

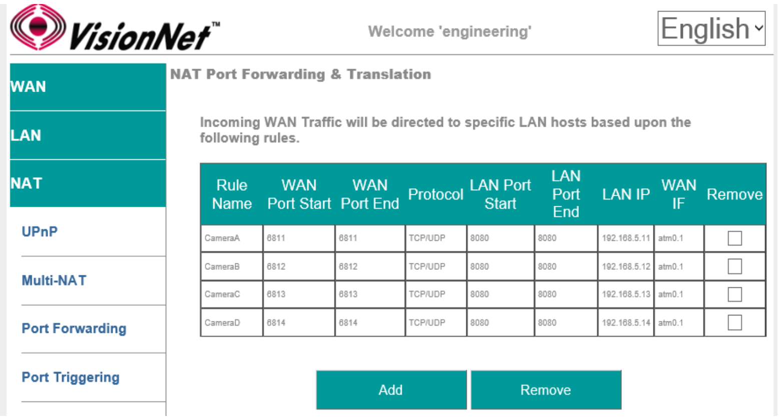
UPnP Configuration

☑ Enable UPnP for NAT Services

**2.B**

**NAT**

**Port Forwarding**



Welcome 'engineering'

NAT Port Forwarding & Translation

Incoming WAN Traffic will be directed to specific LAN hosts based upon the following rules.

| Rule Name | WAN Port Start | WAN Port End | Protocol | LAN Port Start | LAN Port End | LAN IP | WAN IF | Remove |
|---|---|---|---|---|---|---|---|---|
| CameraA | 6811 | 6811 | TCP/UDP | 8080 | 8080 | 192.168.5.11 | atm0.1 | □ |
| CameraB | 6812 | 6812 | TCP/UDP | 8080 | 8080 | 192.168.5.12 | atm0.1 | □ |
| CameraC | 6813 | 6813 | TCP/UDP | 8080 | 8080 | 192.168.5.13 | atm0.1 | □ |
| CameraD | 6814 | 6814 | TCP/UDP | 8080 | 8080 | 192.168.5.14 | atm0.1 | □ |

**Step 3** **When finished, select " Apply / Save ".**

## SECTION 8.2 Multi-NAT

**Abstract**

Once a Routed IPv4 WAN Interface has been created, and NAT Assigned, there may be a need to alter the way that specific applications traverse NAT.

Multi-NAT allows for IP Mapping between public and private IPs.

| | | | |
|---|---|---|---|
| **1:1 NAT:** | 1 LAN IP | ↔ | 1 WAN IP |
| **1: Many NAT:** | 1 LAN IP | ↔ | > 1 WAN IP |
| **Many:1 NAT:** | > 1 LAN IP | ↔ | 1 WAN IP |
| **Many: Many NAT:** | > 1 LAN IP | ↔ | > 1 WAN IP |

Multi-NAT is generally not suggested unless specifically requested by an IT Manager

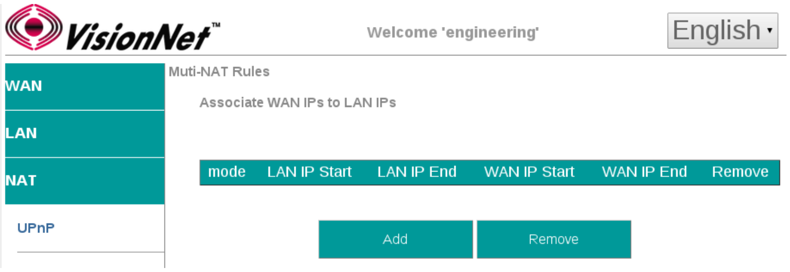
**Step 1** **Direct your browser to the Multi-NAT page**

**1.A** In the left-hand navigation pane, select: **NAT**

**Multi-NAT**

**Step 2** **Create Multi-NAT Rules**

**2.A** **Select “Add”**



Muti-NAT Rules

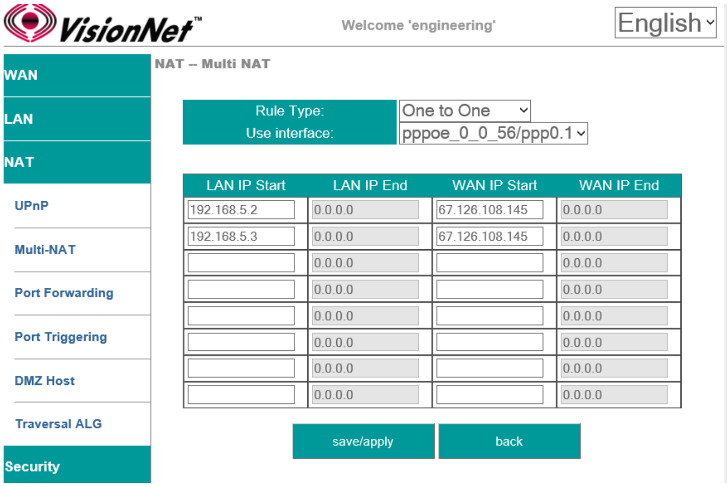
Associate WAN IPs to LAN IPs

| mode | LAN IP Start | LAN IP End | WAN IP Start | WAN IP End | Remove |
|---|---|---|---|---|---|

**2.B** **Rule Type**
**1:1 : 1 LAN IP ↔ 1 WAN IP**
**1: Many : 1 LAN IP ↔ >1 WAN IP**
**Many:1: >1 LAN IP ↔ 1 WAN IP**
**Many: Many : >1 LAN IP ↔>1 WAN IP**

**Use Interface**
WAN interface associated with the rule

**IP Ranges**
Associated with Rule Types



NAT -- Multi NAT

Rule Type: One to One
Use interface: pppoe_0_0_56/ppp0.1

| LAN IP Start | LAN IP End | WAN IP Start | WAN IP End |
|---|---|---|---|
| 192.168.5.2 | 0.0.0.0 | 67.126.108.145 | 0.0.0.0 |
| 192.168.5.3 | 0.0.0.0 | 67.126.108.145 | 0.0.0.0 |
| | 0.0.0.0 | | 0.0.0.0 |
| | 0.0.0.0 | | 0.0.0.0 |
| | 0.0.0.0 | | 0.0.0.0 |
| | 0.0.0.0 | | 0.0.0.0 |
| | 0.0.0.0 | | 0.0.0.0 |
| | 0.0.0.0 | | 0.0.0.0 |

**Step 3** **When finished, select “ Apply / Save “.**

## SECTION 8.3 Port Forwarding

### Abstract

Once a Routed IPv4 WAN Interface has been created, and NAT Assigned, there may be a need to alter the way that specific applications traverse NAT.

Port Forwarding opens ports, on the gateways WAN Interface, and forwards packets destined for those ports to a LAN host.

Port Translation can be specified, if a WAN Port on the gateway is to be forwarded to a different port on the LAN host.

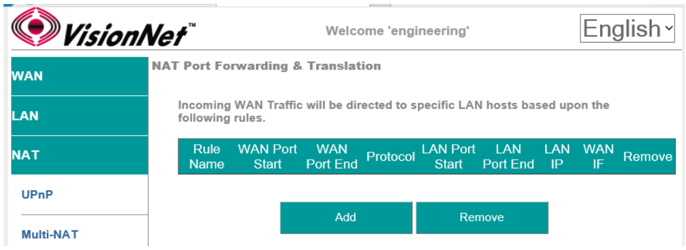
**Step 1** **Direct your browser to the Port Forwarding page**

**1.A** In the left-hand navigation pane, select: **NAT**

**Port Forwarding**

**Step 2** **Create Port Forwarding Rules**

**2.A** **Select “Add”**



NAT Port Forwarding & Translation

Incoming WAN Traffic will be directed to specific LAN hosts based upon the following rules.

| Rule Name | WAN Port Start | WAN Port End | Protocol | LAN Port Start | LAN Port End | LAN IP | WAN IF | Remove |
|---|---|---|---|---|---|---|---|---|

**2.B** **Use Interface**
WAN interface associated with the rule

Service
Use a pre-configured service; or create a custom service.

Custom Service
Provide a unique name

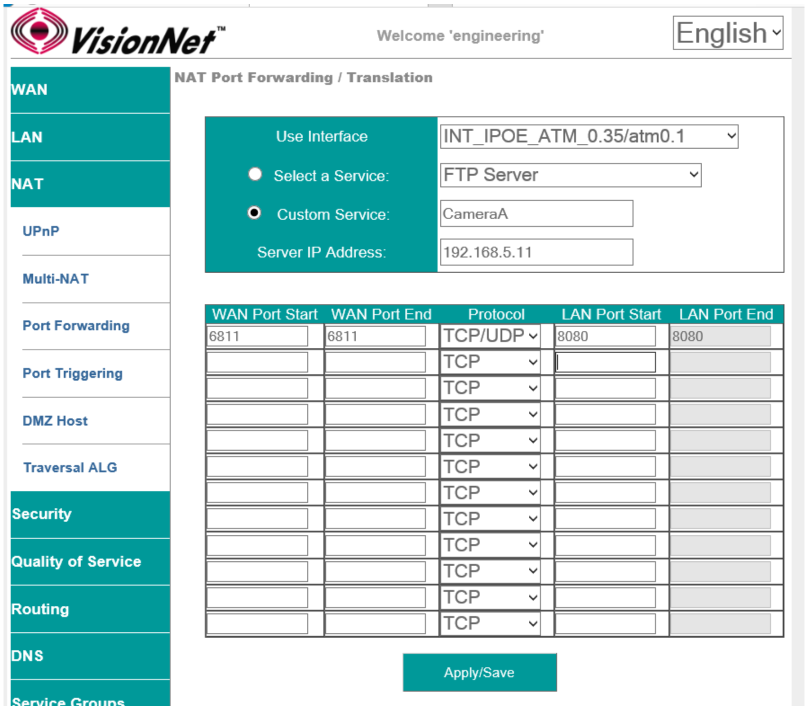
Server IP Address
This is the LAN host’s IP Address

Table Rules
Multiple port associations may be made per rule entry

**WAN Port Start / End**
First and Last ports in entry (ie:6900)

**Protocol**
TCP, UDP, or TCP/UDP

**LAN Port Start / End**
First and Last ports in entry (ie:6900)



NAT Port Forwarding / Translation

| | |
|---|---|
| Use Interface | INT_IPOE_ATM_0.35/atm0.1 |
| ○ Select a Service: | FTP Server |
| ● Custom Service: | CameraA |
| Server IP Address: | 192.168.5.11 |

| WAN Port Start | WAN Port End | Protocol | LAN Port Start | LAN Port End |
|---|---|---|---|---|
| 6811 | 6811 | TCP/UDP | 8080 | 8080 |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |

**Step 3** **When finished, select “ Apply / Save “.**

# SECTION 8.4 Port Triggering

**Abstract**

Once a Routed IPv4 WAN Interface has been created, and NAT Assigned, there may be a need to alter the way that specific applications traverse NAT.

Port Forwarding opens ports, on the gateways WAN Interface, and forwards packets destined for those ports to a LAN host.

Port Translation can be specified, if a WAN Port on the gateway is to be forwarded to a different port on the LAN host.

Port Triggering is a dynamic, host based, port forwarding algorithm. The ports that are opened, and forwarded, are based upon outbound ports utilized by “hosts”. The gateway will then open ports based upon the table rules.

**Step 1** **Direct your browser to the Port Triggering page**

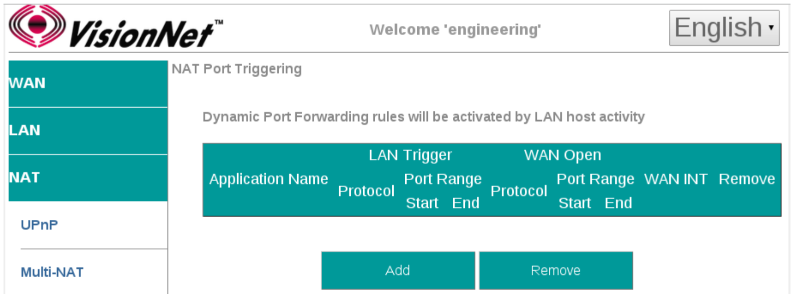
**1.A** In the left-hand navigation pane, select:

**NAT**

**Port Triggering**

**Step 2** **Create Port Triggering Rules**

**2.A** **Select “Add”**



NAT Port Triggering

Dynamic Port Forwarding rules will be activated by LAN host activity

| Application Name | LAN Trigger | | | WAN Open | | | WAN INT | Remove |
|---|---|---|---|---|---|---|---|---|
| | Protocol | Port Range Start | End | Protocol | Port Range Start | End | | |

**2.B** **Use Interface**
WAN interface associated with the rule

Select an Application
Use a pre-configured service; or create a custom service.

Custom Application
Provide a unique name

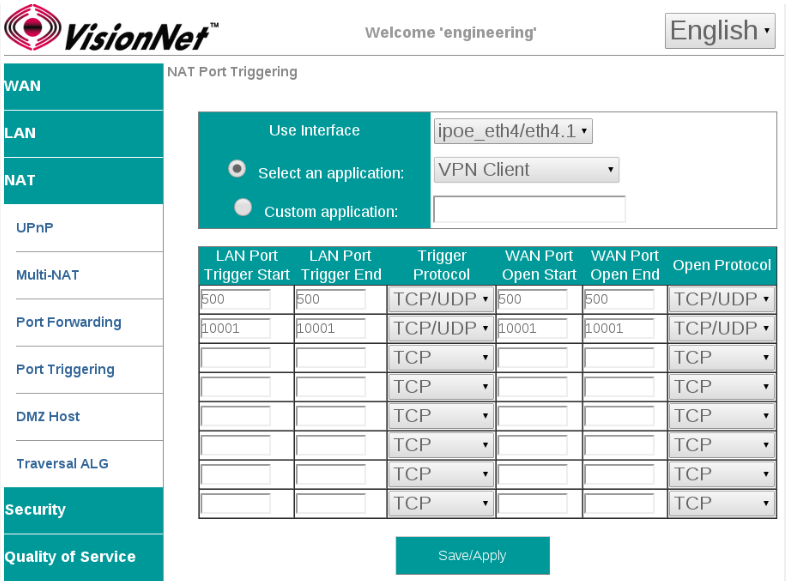
Table Rules

**LAN Port Trigger Start / End**
Port Range requested by host

**Protocol**
TCP, UDP, or TCP/UDP

**WAN Port Start / End**
Port Range opened and forwarded back to host.

**Protocol**
TCP, UDP, or TCP/UDP



NAT Port Triggering

| | |
|---|---|
| Use Interface | ipoe_eth4/eth4.1 |
| ● Select an application: | VPN Client |
| ○ Custom application: | |

| LAN Port Trigger Start | LAN Port Trigger End | Trigger Protocol | WAN Port Open Start | WAN Port Open End | Open Protocol |
|---|---|---|---|---|---|
| 500 | 500 | TCP/UDP | 500 | 500 | TCP/UDP |
| 10001 | 10001 | TCP/UDP | 10001 | 10001 | TCP/UDP |
| | | TCP | | | TCP |
| | | TCP | | | TCP |
| | | TCP | | | TCP |
| | | TCP | | | TCP |
| | | TCP | | | TCP |
| | | TCP | | | TCP |

**Step 3** **When finished, select “ Apply / Save “.**

# SECTION 8.5 DMZ Hosts

**Abstract**

Once a Routed IPv4 WAN Interface has been created, and NAT Assigned, there may be a need to alter the way that specific applications traverse NAT.

DMZ Host forwards all packets, directed to ports not currently associated with a NAT connection, to a single host IP as specified. This is only suggested for trouble-shooting NAT Traversal for applications; but not for permanent use.

**Step 1** **Direct your browser to the DMZ Host page**

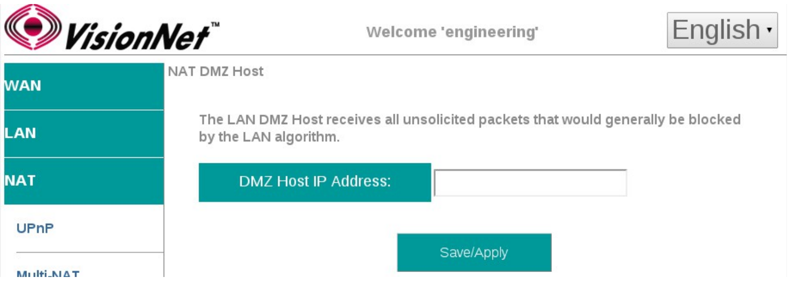
**1.A** In the left-hand navigation pane, select:

**NAT**

**DMZ Host**

**Step 2** **Specify DMZ Host**

**2.A** **Enter the LAN IP of the desired host device**



NAT DMZ Host

The LAN DMZ Host receives all unsolicited packets that would generally be blocked by the LAN algorithm.

DMZ Host IP Address:

Save/Apply

**Step 3** **When finished, select " Apply / Save ".**

## SECTION 8.6 NAT Traversal Algorithms

**Abstract**

Once a Routed IPv4 WAN Interface has been created, and NAT Assigned, there may be a need to alter the way that specific applications traverse NAT.

NAT Traversal algorithms attempt to identify common applications and open up ports to accomodate host / server communications.

Some application clients have evolved to traverse NAT without need for these algorithms. If there is an unresolved issue, involving NAT, you may wish to begin by disabling all algorithms and then enable specific protocols.

Up to 40 NAT Traversal connections may be concurrently utilized.

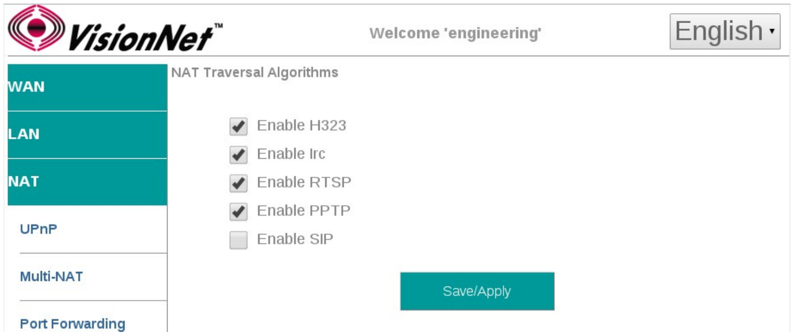
**Step 1 Direct your browser to the Traversal ALG page**

**1.A** In the left-hand navigation pane, select: **NAT**

**Traversal ALG**

**Step 2 Enable / Disable requested ALG**

**2.A Enter the LAN IP of the desired host device**



NAT Traversal Algorithms

☑ Enable H323
☑ Enable Irc
☑ Enable RTSP
☑ Enable PPTP
□ Enable SIP

Save/Apply

**Step 3 When finished, select " Apply / Save ".**

# SECTION 9: WiFi Configuration

## SECTION 9.1 Enable / Disable WiFi

**Abstract:**

WiFi may be enabled / disabled

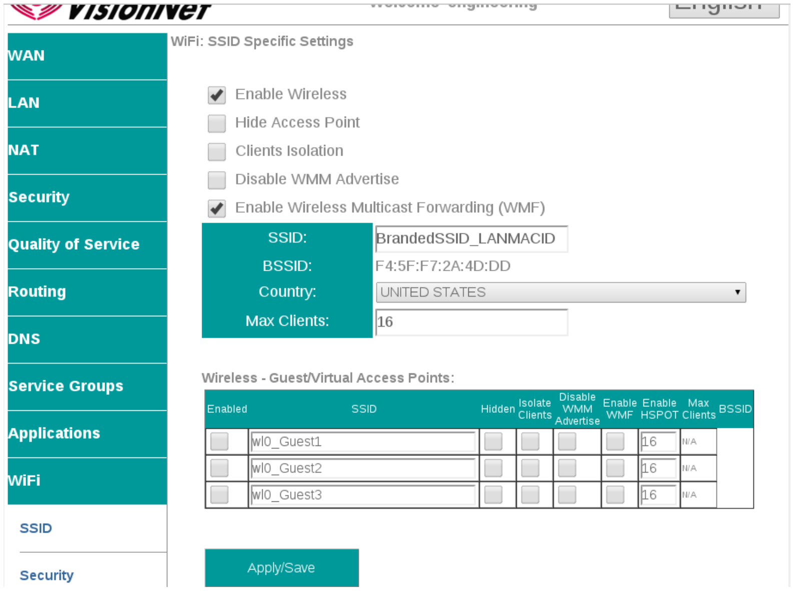
**Step 1** **Direct your browser to the SSID page**

**1.A** In the left-hand navigation pane, select: **WiFi**

**SSID**

**Step 2** **Enable / Disable WiFi**

**2.A** Check / Uncheck the box labeled **"Enable Wireless"**



WiFi: SSID Specific Settings

☑ Enable Wireless
☐ Hide Access Point
☐ Clients Isolation
☐ Disable WMM Advertise
☑ Enable Wireless Multicast Forwarding (WMF)

| | |
|---|---|
| SSID: | BrandedSSID_LANMACID |
| BSSID: | F4:5F:F7:2A:4D:DD |
| Country: | UNITED STATES |
| Max Clients: | 16 |

Wireless - Guest/Virtual Access Points:

| Enabled | SSID | Hidden | Isolate Clients | Disable WMM Advertise | Enable WMF | Enable HSPOT | Max Clients | BSSID |
|---|---|---|---|---|---|---|---|---|
| ☐ | wl0_Guest1 | ☐ | ☐ | ☐ | ☐ | 16 | N/A | |
| ☐ | wl0_Guest2 | ☐ | ☐ | ☐ | ☐ | 16 | N/A | |
| ☐ | wl0_Guest3 | ☐ | ☐ | ☐ | ☐ | 16 | N/A | |

**Step 3** **When finished, select " Apply / Save ".**

**It may take up to 1 minute for your change to take effect**

# SECTION 9.2 Configure SSID Specific Settings

**Abstract:**

SSID Specific settings may be altered for optimized interoperability

**Step 1** **Direct your browser to the SSID page**

**1.A** In the left-hand navigation pane, select: **WiFi**

**SSID**

**Step 2** **SSID Related Settings**

**2.A** ENABLE WIRELESS

**This enables / Disables WiFi services**

HIDE ACCESS POINT

If this is selected, the SSID name will not be broadcasted

CLIENTS ISOLATION

This prevents ad-hoc networks; but could impede upon some applications (ie: printing)

Disable WMM Advertise

**WMM is required for modern MultiMedia applications. Disable only for support of legacy devices. This will lower aggregate speed**

Enable WMF

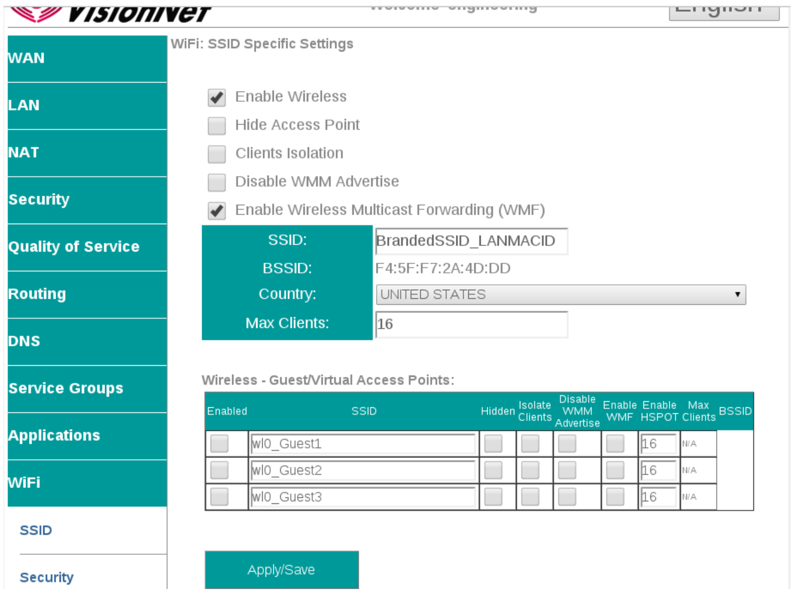
**Wireless Multicast Forwarding is useful for modern Media Sharing applications**

SSID Name

This is the broadcasted SSID name

Virtual / Guest networks

Mutliple SSIDs may be broadcasted (ie: temporary access). Clients will operate on the primary LAN



WiFi: SSID Specific Settings

☑ Enable Wireless
☐ Hide Access Point
☐ Clients Isolation
☐ Disable WMM Advertise
☑ Enable Wireless Multicast Forwarding (WMF)

| | |
|---|---|
| SSID: | BrandedSSID_LANMACID |
| BSSID: | F4:5F:F7:2A:4D:DD |
| Country: | UNITED STATES |
| Max Clients: | 16 |

Wireless - Guest/Virtual Access Points:

| Enabled | SSID | Hidden | Isolate Clients | Disable WMM Advertise | Enable WMF | Enable HSPOT | Max Clients | BSSID |
|---|---|---|---|---|---|---|---|---|
| ☐ | wl0_Guest1 | ☐ | ☐ | ☐ | ☐ | 16 | N/A | |
| ☐ | wl0_Guest2 | ☐ | ☐ | ☐ | ☐ | 16 | N/A | |
| ☐ | wl0_Guest3 | ☐ | ☐ | ☐ | ☐ | 16 | N/A | |

**Step 3** **When finished, select " Apply / Save ".**

## It may take up to 1 minute for your change to take effect

# SECTION 9.3 WiFi Security

**Abstract:**

WiFi Security should always be enabled. The following directions will provide detail on configuration.

**Step 1** **Direct your browser to the SSID page**

**1.A** In the left-hand navigation pane, select: **WiFi**

**Security**

**Step 2** **SSID Related Security Settings**

**2.A** **Enable WPS**
Suggested Configuration - Disabled

**SSID**
Select SSID

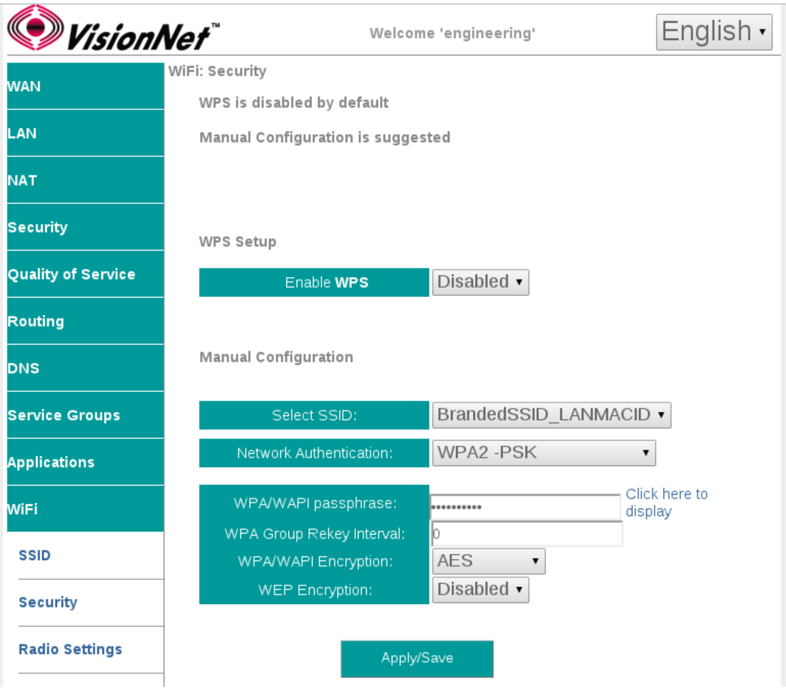
**Network Authentication**
Suggested Setting: WPA2-PSK

**WPA Passphrase**
This may be any passphrase that you like.

**WPA Group Rekey Interval**
Suggested Setting: 0

**WPA Encryption**
Suggested Setting: AES

**WEP Encryption**
Suggested Setting: Disabled



WiFi: Security

WPS is disabled by default

Manual Configuration is suggested

WPS Setup

Enable WPS: Disabled

Manual Configuration

Select SSID: BrandedSSID_LANMACID

Network Authentication: WPA2 -PSK

WPA/WAPI passphrase: ••••••••••

WPA Group Rekey Interval: 0

WPA/WAPI Encryption: AES

WEP Encryption: Disabled

**Step 3** **When finished, select “ Apply / Save “.**

**It may take up to 1 minute for your change to take effect. You will need to “forget” old network settings and re-connect all devices after making this change.**

# SECTION 9.4  WiFi Radio Settings

**Abstract:**

Most radio settings should be left as default. Below, are key settings for optimizing performance.

## Step 1 Direct your browser to the SSID page

**1.A** In the left-hand navigation pane, select: **WiFi**

**Radio Settings**

## Step 2 SSID Related Security Settings

**2.A**

**Band:**
This device only supports 2.4Ghz

**Channel:**
Auto will allow the device to auto-select a channel. This will also allow the WiFi button, located on the top front of the device, to change the channel.

**802.11n/EWC**
Suggested Setting: Auto

**802.11n Auto**
Suggested Setting: Auto

**802.11n Protection**
Suggested Setting: Off

**802.11n Client Only**
Suggested Setting: Off

**RIFS Advertisment**
Suggested Setting: Auto

**OBSS Coexistence**
Suggested Setting: Enabled

**RX Chain Power Save**
Suggested Setting: Disabled

**RX Chain Power Save Quiet Time:**
Suggested Setting: 10

**RX Chain Power Save PPS:**
Suggested Setting: 10

**54g Rate**
Suggested Setting:1Mbps

**Multicast Rate**
Suggested Setting: Disabled

**Basic Rate**
Suggested Setting: Default

**Fragmentation Threshold**
Suggested Setting: 2346

**RTS Threshold**
Suggested Setting: 2347

**DTIM Threshold**
Suggested Setting: 1

**Beacon Interface**
Suggested Setting: 100

**Global Max Clients:**
Suggested Setting: 16

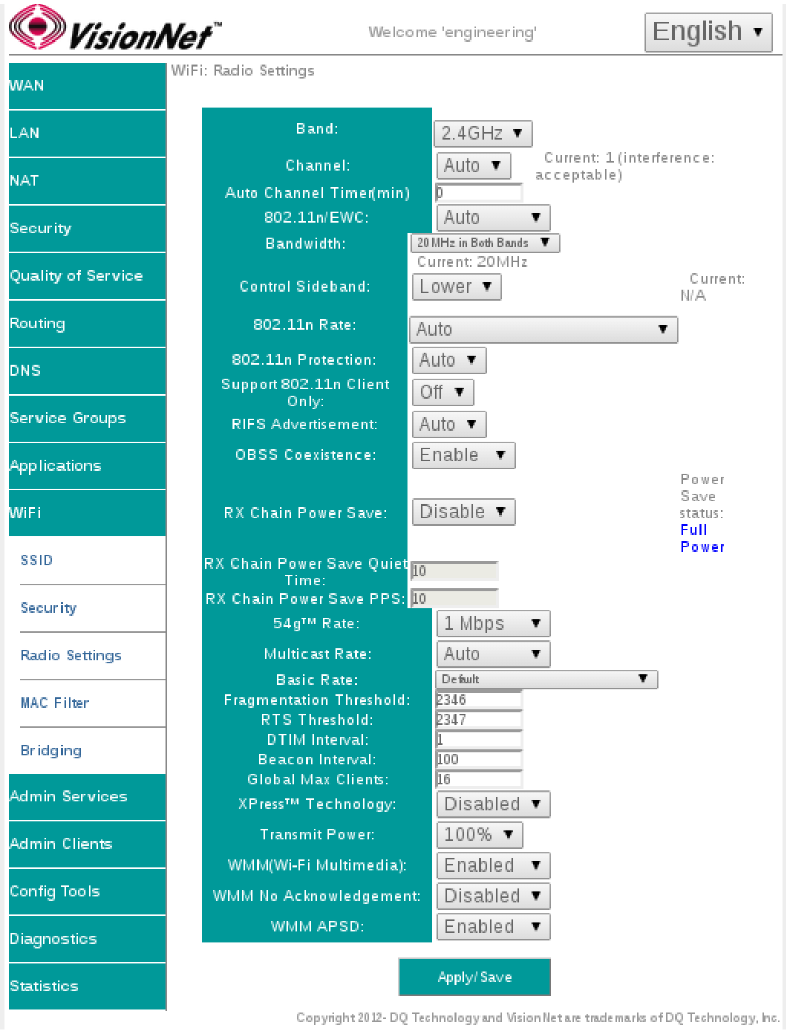
**Xpress Technology**
Suggested Setting: Disabled

**Transmit Power**
Suggested Setting: 100%

**WMM**
Suggested Setting: Enabled

**WMM No Acknowledgement**
Suggested Setting: Disabled

**WMM APSD**
Suggested Setting: Enabled



Welcome 'engineering'

WiFi: Radio Settings

| | |
|---|---|
| Band: | 2.4GHz |
| Channel: | Auto — Current: 1 (interference: acceptable) |
| Auto Channel Timer(min) | 0 |
| 802.11n/EWC: | Auto |
| Bandwidth: | 20 MHz in Both Bands — Current: 20MHz |
| Control Sideband: | Lower — Current: N/A |
| 802.11n Rate: | Auto |
| 802.11n Protection: | Auto |
| Support 802.11n Client Only: | Off |
| RIFS Advertisement: | Auto |
| OBSS Coexistence: | Enable |
| RX Chain Power Save: | Disable — Power Save status: Full Power |
| RX Chain Power Save Quiet Time: | 10 |
| RX Chain Power Save PPS: | 10 |
| 54g™ Rate: | 1 Mbps |
| Multicast Rate: | Auto |
| Basic Rate: | Default |
| Fragmentation Threshold: | 2346 |
| RTS Threshold: | 2347 |
| DTIM Interval: | 1 |
| Beacon Interval: | 100 |
| Global Max Clients: | 16 |
| XPress™ Technology: | Disabled |
| Transmit Power: | 100% |
| WMM(Wi-Fi Multimedia): | Enabled |
| WMM No Acknowledgement: | Disabled |
| WMM APSD: | Enabled |

Copyright 2012- DQ Technology and VisionNet are trademarks of DQ Technology, Inc.

## Step 3 When finished, select " Apply / Save ".

**It may take up to 1 minute for your change to take effect.**

# SECTION 10: Product Specifications

## SECTION 10.1 Product Specifications

**WAN Interface Features**
- T1.413
- G.Lite
- G.DMT
- ADSL2 / ADSL2+
- SRA
- Bitswap
- AAL5, UNI 3.1/4, F4/F5
- Annex A
- Annex L
- Annex M
- PhyR / G.INP
- Nitro
- PTM
- ATM
- Ethernet
- Adjustable MTU
- UBR/CBR/VBR-rt/nrt

**LAN Service Features**
- Inter LAN Routing
- Multiple DHCP Servers
- Multi-Option DHCP
- MAC Reservation
- UPnP
- IPv4, IPv6, Dual Stack
- Isolated LAN Networks
- Service Grouping
- Secondary Subnetting
- IGMP Snoop / Block
- IPTV Acceleration
- Enhanced IGMP
- IGMP Customization
- IGMP QoS
- QoS: IP, MAC, ToS, DSCP, 802.1p, Src/Dest, ATM

**WAN Service Features**
- Bridge
- IPoE
- VLAN MUX / Tagging
- IPv4, IPv6
- PPPoE (PAP,CHAP,Auto) • IGMP Proxy/Multi-cast
- PPPoA
- PPP IP Extension
- IPoA
- ATM QoS, FWQ, MPAAL
- Group Specific Routing • ATM Priority Queing
- Multi-Protocol Encapsulation
- Multiple Services Connection
- Multi-Option DHCP

**Security / Routing Features**
- NAT / NAPT / SPI
- DoS Attack Prevention
- Bridge Filtering
- VPN Pass-Through
- Port Forwarding
- Port Triggering
- IP Incoming/Outgoing
- QoS Parameter Table
- ALG Control
- Routable LAN / DMZ
- IP and URL Filtering
- Time of Day Filtering
- Dynamic DNS
- IPSEC VPN Tunneling
- RIP V1, V2
- Static and Policy Routing

**Diagnostic Features**
- WAN Quick View
- ATM Diagnostics
- DSL Diagnostics
- Ping / Trace Route
- System Log
- DNS Path Verification
- Tiered GUI Interface
- SNTP Client
- Isolated LAN Networks
- Remote Access Security
- End User GUI
- Customer Support GUI

**Wi Fi Features**
- 802.11b/g/n 2T2R
- 2.4Ghz 20/40Mhz
- 17dBm
- Qty 2 -3 dbi RP-SMA
- WEP, WPA, WPA2, PSK
- AES, TKIP
- 802.1x Radius Support
- WPS
- 1 Main, 3 Guest SSIDs
- WMM, WAPSD, QoS
- UMA Mobile Converge

Management Protocols
- HTTP
- Telnet
- SSH
- TFTP
- ACS / TR-069
- SNMP

**Hardware Specifications**
**WAN:** xDSL, Ethernet (Omni-Port LAN or WAN)

**LAN: Switch A: 4 Port Fast Ethernet**

**USB:** 2.0 Type A - DLNA, Samba, Wireless Uplink

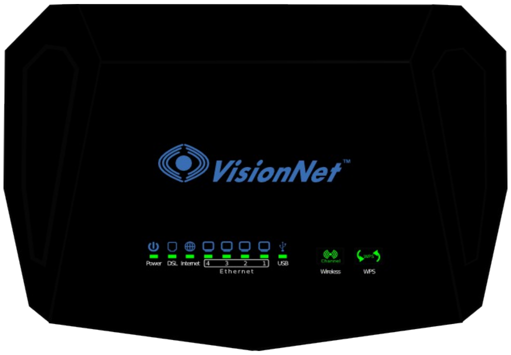
**WiFi:** 802.11b/g/n - 2.4Ghz

**Power:** 12VDC / 110-220VAC, 50~60Hz

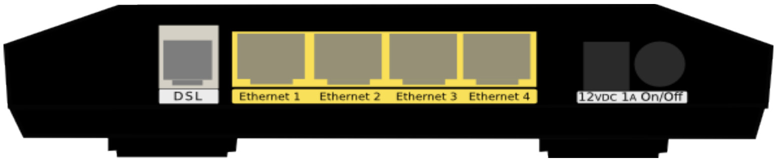
**Temp:** 0 - 65C, Humidity: 5 ~ 95% (non-condensing)

# SECTION 10.2 Product Depictions

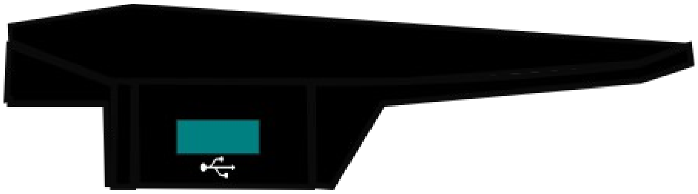
## Front Depiction



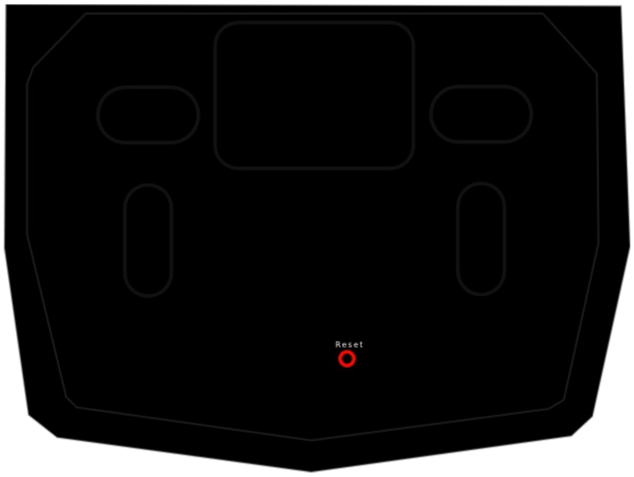
## Back Depiction



## Top Depiction



## Bottom Depiction



## SECTION 10.3 LED Functionality

| Label | Description | Functionality |
|---|---|---|
| Power | Status Power / Router | Solid Green – Power On<br>Off – Power Off<br>Flashing Green 2 hz – Flashing Power on self test<br>Flashing Red 4 hz- Failure (not bootable) or device malfunction<br>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 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. |
| Ethernet 1 | Status Ethernet Port | Off - Power Off – or – No Powered device detected<br>Solid Green – Powered device connected ; including wake on LAN<br>Flashing Green – LAN activity present for that port |
| Ethernet 2 | Status Ethernet Port | Off - Power Off – or – No Powered device detected<br>Solid Green – Powered device connected ; including wake on LAN<br>Flashing Green – LAN activity present for that port |
| Ethernet 3 | Status Ethernet Port | Off - Power Off – or – No Powered device detected<br>Solid Green – Powered device connected ; including wake on LAN<br>Flashing Green – LAN activity present for that port |
| Ethernet 4 | Status Ethernet Port | Off - Power Off – or – No Powered device detected<br>Solid Green – Powered device connected ; including wake on LAN<br>Flashing Green – LAN activity present for that port<br>LED Location specifies Link Status 10 / 100 / GbE |
| Wireless | Status WiFi | Off - Modem off or Wireless not activated<br>Solid Green – Wireless activated<br>Flashing Green 2 hz– WPS Activated – Association Period<br>Flashing Green 4 Hz - Wireless Activity<br><br>Note: Pressing the WiFi button enables a re-scan of the WiFi Spectrum |
| WPS | Status WPS | Off: WPS Not in use<br>Solid Green: Devices authenticated via WPS<br>Flashing Green: WPS authenticated activated, authenticating devices<br><br>Note: Presseing the WPS button enables WPS if enabled in the GUI |
| DSL | Status DSL Link Line 1 | Green – DSL Good Sync<br>Off - Powered off<br>Flashing Green - DSL Attempting sync<br>Signal Detection – Flashing 2hz with 50% duty cycle<br>Carrier Detected, Modem training – Flashing at 4hz with 50% duty cycle |
| Internet | Status Internet Connection | Internet Light – Must indicate at least one type of connection<br>Solid Green – IP connected – no traffic passing<br>Device has a WAN IP via either static/ DHCP/ or IPCP<br>If PPP is used, device has authenticated and has a WAN IP Address<br>If IP or PPPOE session is idle and dropped, light to remain green as long as ADSL is still present. Light to turn red if upon attempting new session it fails.<br>Off – Modem Power Off.<br>LED Should remain off if modem is in bridged mode or if DSL Connection is not present<br>Flashing Green – Device has WAN IP Address and IP Traffic is passing through device<br>Red – Device attempted initiate session, either authentication or to obtain an IP Address, and failed. an IP Address, and failed. |

## SECTION 10.4 Regulatory Advisories

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

**VisionNet**
**Model: M505N**
**FCC ID: QMPM505NR3 US: DQ1DL01BM505NR3**

**This device complies with part 15 of the FCC Rules.**
**Operation is subject to the following two conditions:**
**(1) This device may not cause harmful interference and**
**(2) this device must accept any interference received, including interference that may cause undesired operation.**

**This device complies with FCC part 68 Rules.**

**IMPORTANT NOTE:**

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 centimeters between the radiator and your body.

This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may case harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

## Customer Information

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

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

3. If this equipment [US: DQ1DL01BM505NR3] causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

4. The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

5. If trouble is experienced with this equipment [US: DQ1DL01BM505NR3], for repair or warranty information, Service can be facilitated through our office at:

U.S. Agent Company name: DQ Technology, Inc.
Address: 5111 Johnson Drive, Pleasanton, CA 94588, USA
Telephone: +1 925 730 3940
Email: support@visionnetusa.com

If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

6. Please follow instructions for repairing if any (e.g. battery replacement section); otherwise do not alternate or repair any parts of device except specified. For repair procedures, follow the instructions outlined under the limited warranty.

7. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

8. If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this equipment does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

9. If the telephone company requests information on what equipment is connected to their lines, inform them of:

a) The ringer equivalence number[ 0.1B]
b) The USOC jack required [RJ11C]
c) Facility Interface Codes ("FIC") [METALLIC]
d) Service Order Codes ("SOC") [9.0Y]
e) The FCC Registration Number [US: DQ1DL01BM505NR3]

10. The REN is used to determine the number of devices that may be connected to a telephone line.

Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs  should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. The REN for this product is part of the product identifier that has the format US: AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point. For this product, the FCC Registration number [US: DQ1DL01BM505NR3] indicates the REN would be. 0.1.

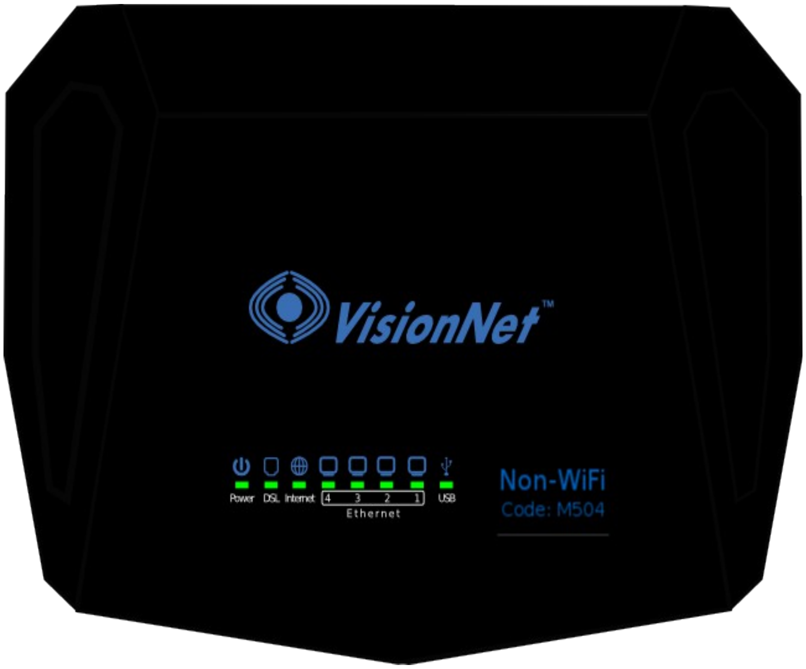
# SECTION 10.5 M504  / M505N Distinctions

Abstract:

The M504 as an exclusive model has been deprecated; but VisionNet is providing a customized product to legacy customers. The following modifications are being made to the M505N for this particular use case.

**Wireless is Disabled in the Firmware**
a license will be made available for purchase, in which VisionNet can remotely enable Wireless on a device

**Wireless LEDs / Buttons are covered by a designation label**
a license will be made available for purchase, in which VisionNet can remotely enable Wireless on a device



# SECTION 10.6 M504 / M505N Distinctions

**Abstract:**

The M50x has a “Primary WAN MAC” located on the bottom of each modem. The gateway allocates WAN MAC Addresses, for each interface, based upon incremental priority from the primary WAN MAC.

The priority, at initial IF scan, is as follows

| Priority | IF | Notes |
|---|---|---|
| Primary | ETHERNET | +0 If Present.<br>Each subsequent VLAN is assigned +1 hex digit |
| Secondary | PTM | +0 If No ETH Present.<br>Initial VLAN is assigned +1 hex digit.<br>Each subsequent VLAN Assigned +1 Hex digit. |
| Tertiary | ATM | +0 If No ETH or PTM Present.<br>Initial VLAN is assigned +1 hex digit.<br>Each subsequent VLAN Assigned +1 Hex digit. |

**Examples:**

**Expanded IF Example**

| IF | Hex Digit | Example | IF Type |
|---|---|---|---|
| LAN | 0 | N/A | N/A |
| WAN Base A | +2 | Ethernet 4 Untagged (Reserved if VLANs used) | ETHERNET |
| WAN Base A: VLAN A | +3 | Ethernet 4 VLAN 100 | |
| WAN Base A: VLAN B | +4 | Ethernet 4 VLAN 101 | |
| WAN Base B | +5 | PTM 0 | PTM |
| WAN Base B: VLAN A | +6 | PTM 0.1: VLAN Null Tag | |
| WAN Base B: VLAN B | +7 | PTM 0.2: VLAN 101 | |
| WAN Base C | +8 | ATM 0 | ATM |
| WAN Base C: VLAN A | +9 | ATM 0.1: PVC 0/35 VLAN Null Tag | |
| WAN Base D | +10 | ATM 1 | ATM |
| WAN Base D: VLAN A | +11 | ATM 1.1: PVC 0/36 VLAN Null Tag | |

**Single ATM Example**

| IF | Hex Digit | Example | IF Type |
|---|---|---|---|
| LAN | 0 | N/A | N/A |
| WAN Base A | +2 | ATM 0 | ATM |
| WAN Base A: VLAN A | +3 | ATM 0.1: PVC 0/35 VLAN Null Tag | |

### Multiple ATM Example

| IF | Hex Digit | Example | IF Type |
|---|---|---|---|
| LAN | 0 | N/A | N/A |
| WAN Base A | +2 | ATM 0 | ATM |
| WAN Base A: VLAN A | +3 | ATM 0.1: PVC 0/35 VLAN Null Tag | |
| WAN Base B | +4 | ATM 1 | ATM |
| WAN Base B: VLAN A | +5 | ATM 1.1: PVC 0/36 VLAN Null Tag | |

### PTM / ATM Example

| IF | Hex Digit | Example | IF Type |
|---|---|---|---|
| LAN | 0 | N/A | N/A |
| WAN Base A | +2 | PTM 0 | PTM |
| WAN Base A: VLAN A | +3 | PTM 0.1: VLAN Null Tag | |
| WAN Base A: VLAN B | +4 | PTM 0.2: VLAN 101 | |
| WAN Base B | +5 | ATM 0 | ATM |
| WAN Base B: VLAN A | +6 | ATM 0.1: PVC 0/35 VLAN Null Tag | |
| WAN Base D | +7 | ATM 1 | ATM |
| WAN Base D: VLAN A | +8 | ATM 1.1: PVC 0/36 VLAN Null Tag | |

### ETHERNET / ATM Example

| IF | Hex Digit | Example | IF Type |
|---|---|---|---|
| LAN | 0 | N/A | N/A |
| WAN Base A | +2 | Ethernet 4 Untagged | ETHERNET |
| WAN Base B | +3 | ATM 0 | ATM |
| WAN Base B: VLAN A | +4 | ATM 0.1: PVC 0/35 VLAN Null Tag | |