



Product Manual

Model: M625N R1

Product Description: Broadband Gateway

WAN:	Bonded VDSL2 / ADSL2+ / Ethernet WAN
Ethernet:	Qty 2 - Gbe Ethernet, Qty 3 - 10/100 Ethernet
USB:	2.0 (Media Share / Wireless Uplink)
WiFi:	802.11 b/g/n 2T2R 2.4Ghz

Table of Contents

SECTION 1: MANAGEMENT ACCESS

1.1	UNDERSTANDING YOUR DOCUMENTATION	6
1.2	MANAGEMENT ACCOUNTS	7
1.3	SERVICE SECURITY CONSIDERATIONS	8
1.4	GUI ACCESS	9
1.5	CLI ACCESS	10

SECTION 2: WAN CONFIGURATION

2.1	WAN LOGIC OVERVIEW	11
2.2	X DSL LOGIC	14
2.3	CUSTOMIZING X DSL PARAMETERS	16
2.4	DEFINING PHYSICAL WAN PORT OPERATION	17
2.5	CREATING AN ATM INTERFACE	18
2.6	CREATING A PTM INTERFACE	20
2.7	CREATING AN ETHERNET INTERFACE	21
2.8	CREATE/MODIFY A BRIDGED WAN SERVICE	22
2.9	CREATE/MODIFY AN IPOE WAN SERVICE	24
2.10	CREATE/MODIFY A PPP WAN SERVICE	28

SECTION 3: QUALITY OF SERVICE

3.1	QUALITY OF SERVICE ENABLE/DISABLE	32
3.2	INTERFACE CONFIGURATION	33
3.3	QOS CLASSIFICATION TABLE	34

SECTION 4: SERVICE GROUPS

4.1	SERVICE GROUP LOGIC	35
4.2	SERVICE GROUP CREATION	36

SECTION 5: IPv4 LAN CONFIGURATION

5.1	IPv4 CONFIGURATION	37
5.2	IGMP MULTICAST	38

SECTION 6: IPv4 ROUTE CONFIGURATION

6.1	GATEWAY PRIORITIZATION	39
-----	------------------------	----

6.2	STATIC ROUTE TABLE	40
6.3	POLICY ROUTE TABLE	41

SECTION 7: IPv4 DNS CONFIGURATION

7.1	GLOBAL DNS PRIORITIZATION	42
7.2	STATICALLY ASSIGNED GLOBAL DNS	43

SECTION 8: IPv4 NAT TRAVERSAL

8.1	UPnP	42
8.2	MULTI-NAT	43
8.3	PORT FORWARDING	46
8.4	PORT TRIGGERING	47
8.5	DMZ HOSTS	48
8.6	NAT TRAVERSAL ALGORITHM	49

SECTION 9: WIFI CONFIGURATION

9.1	ENABLE/DISABLE WIFI	50
9.2	CONFIGURE SSID SPECIFIC SETTINGS	51
9.3	WIFI SECURITY	52
9.4	WIFI RADIO SETTINGS	53

SECTION 10: PRODUCT SPECIFICATION

10.1	PRODUCT SPECIFICATION	54
10.2	PRODUCT DEPICTION	55
10.3	LED FUNCTIONALITY	56
10.4	REGULATORY ADVISORIES	57
10.5	Firmware Release Notes	60

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.

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

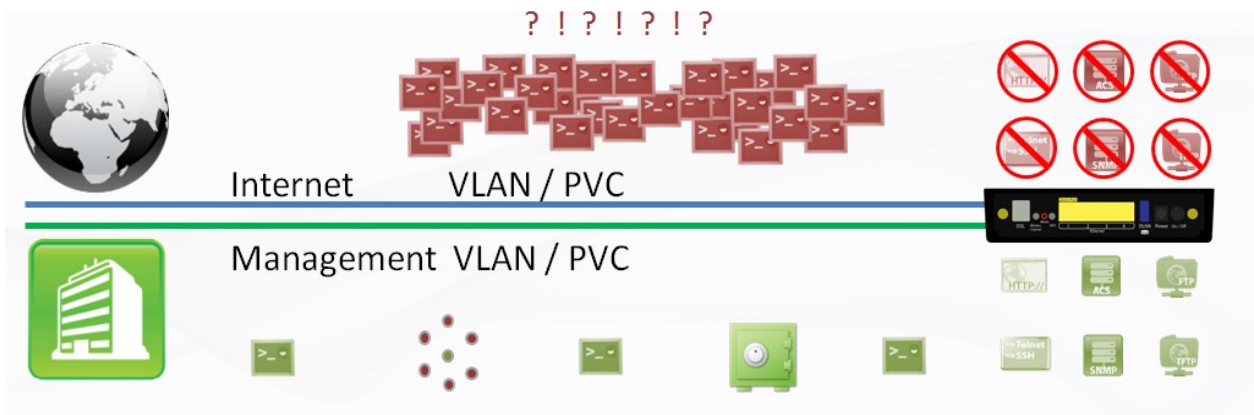
Use of Non-Standard ports help ensure consistency in an environment where UPnP, and customer port forwarding, may re-map standard ports for personal use.

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.

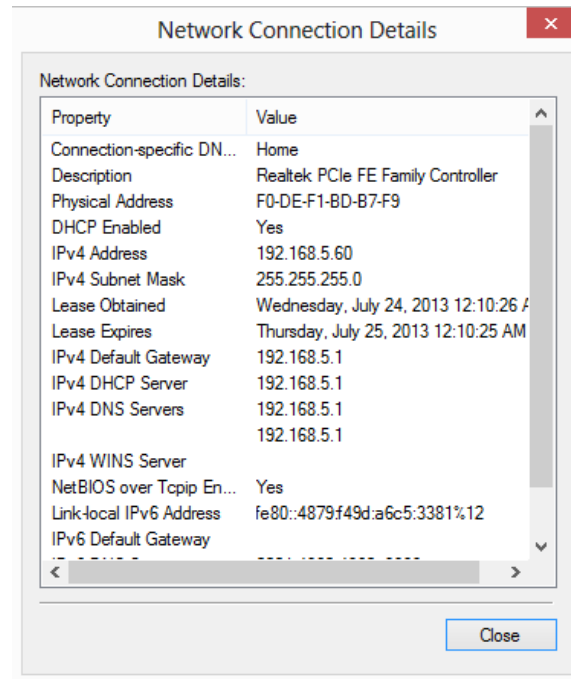
Verify that your local IP will not be blocked by any gateway, or network, ACLs.

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.



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.

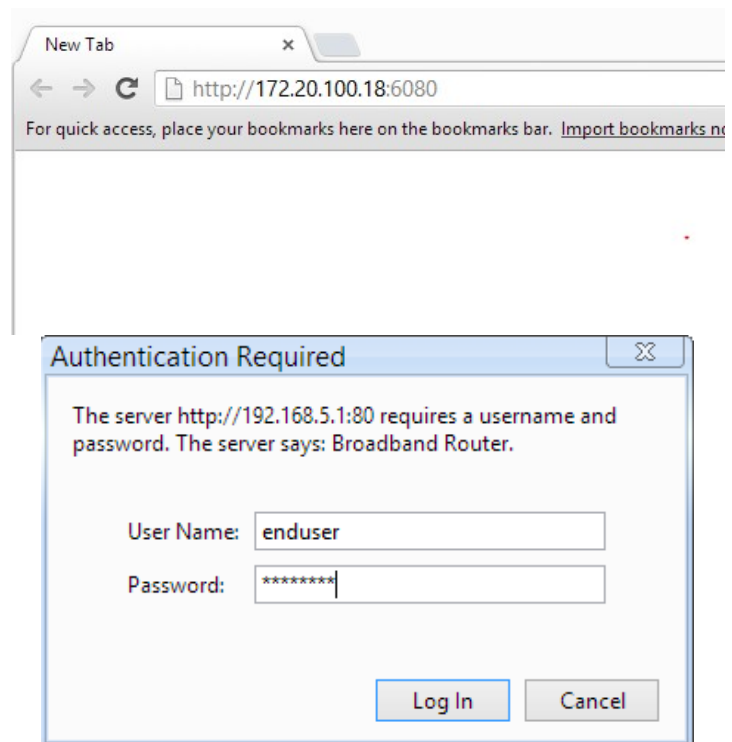
Example of WAN Access:

http://172.20.100.18:6080

Example of LAN Access:

http://192.168.6.1

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



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.

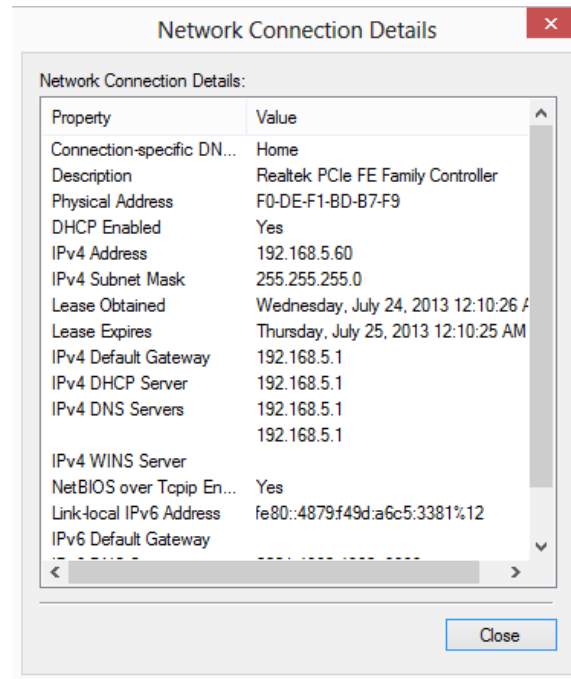
Verify that your local IP will not be blocked by any gateway, or network, ACLs.

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.



Step 2 Connect via Client

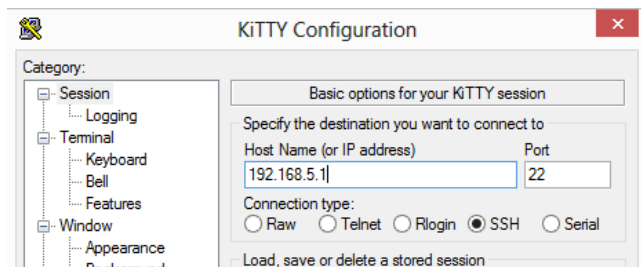
- 2.A Via your OS Terminal, or Console Program, you may enter the IP and Port information

Example of WAN Access:

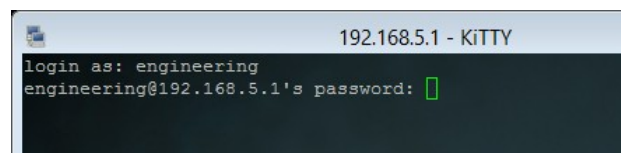
172.20.100.18 port 6022

Example of LAN Access:

192.168.6.1 port 22



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



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

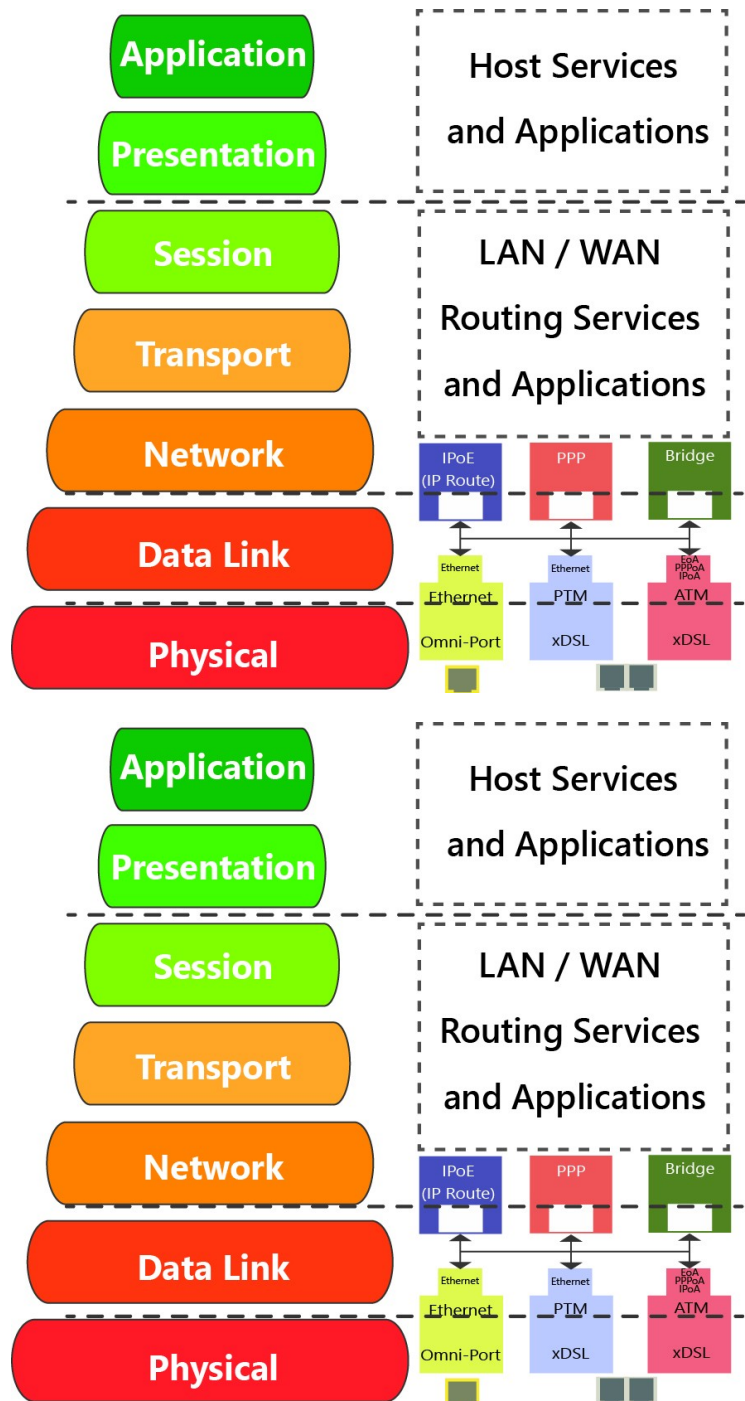
Bridged
Available for: ATM, PTM, ETH
Passes Traffic – No Routing

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

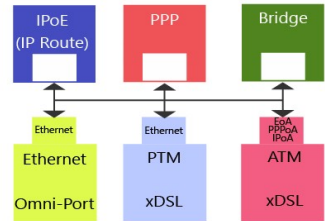
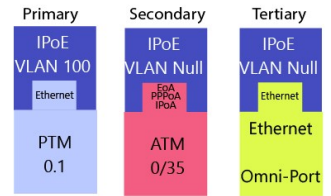
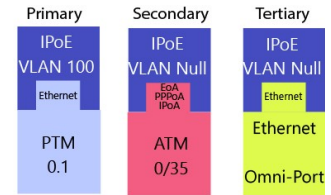
- 1: Add & Define WAN Interface**
ATM
PTM
ETH (Omni-Port)
- 2: Add and Define Service to Interface**
ATM
PTM
ETH (Omni-Port)
- 3: Prioritize for Default Service Group**
Gateway
DNS
- 4: Add Service Group**
If Applicable

4: Add Service Group
(If Applicable)

3: Prioritize Gateway and
DNS Paths

2: Add Service to Interface

1: Create Interface



2.B Tearing Down WAN Services

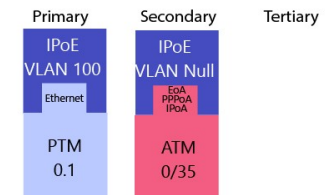
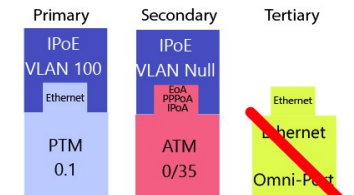
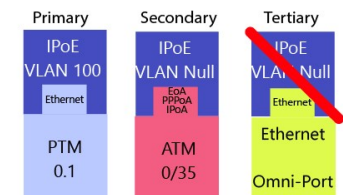
WAN Services Must be removed as follows:

- 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

1: Remove Service

2: Remove Interface

3: Remove Service Group
(If Applicable)



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.



Option 1: xDSL Only



Option 2: Omni-Port WAN Only



Option 3: Activate Omni-Port on timeout

SECTION 2.2 xDSL LOGIC

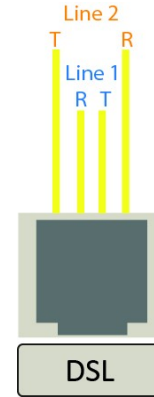
Item 1 xDSL Physical Interfaces

1.A xDSL Port Bonding Layout

Line Pinout

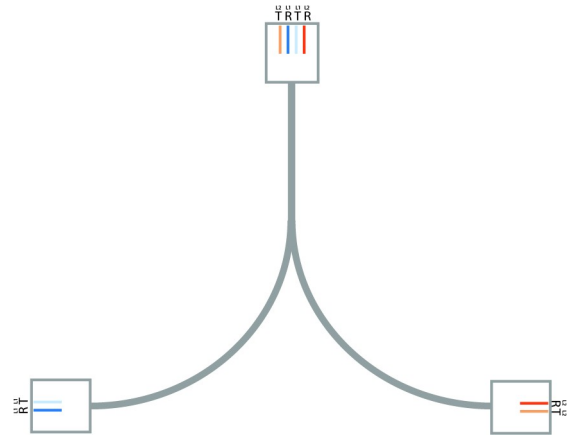
The CPE does not have a preference regarding which line, in a bonding group, is primary or secondary when G.BOND is enabled

The CPE is designed to operate on one line only, if the other is not connected or is disconnected.



1.B xDSL Line Cord Preferences

VisionNet provides a dual ended, low cross-talk assembled cable with the M625N.



Item 2 xDSL Bonding / xDSL Operation

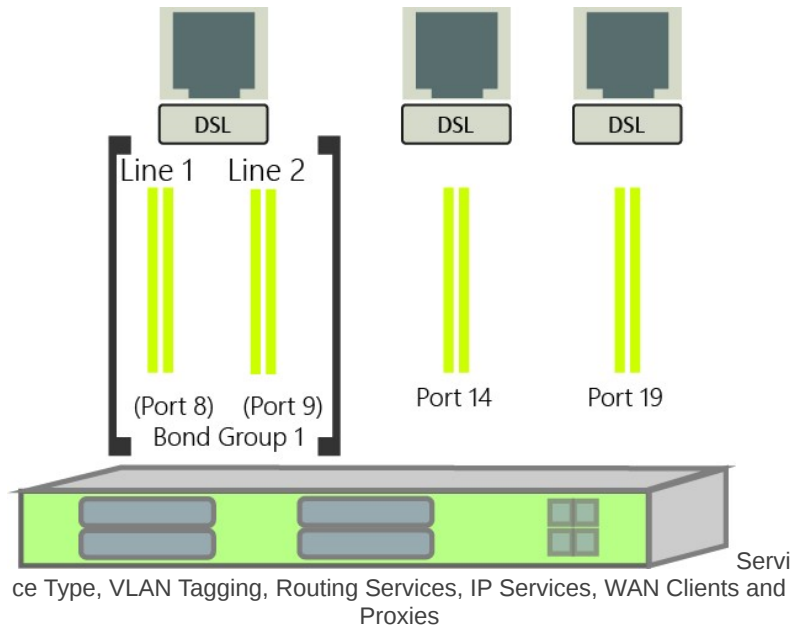
2.A Bonded Operation

G.Bond is simply a method of bandwidth aggregation.

The DSLAM providing services must support bonding; and must have both service lines within the same, isolated, bonding group.

By default, the CPE does not differentiate between line 1 and 2; and will consider the xDSL interface to be one WAN connection.

The addition of a second line only increases the aggregate bandwidth.



2.B ADSL2+ / VDSL2 Associations

VDSL2

Operating Frequency:
8 to 30 Mhz

MaxSpeed:
100Mbps DS, 100Mbps US

General Operation:
PTM – (ATM limits speed)

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
VDSL2 8a	G.994.2	8.832
VDSL2 8b	G.994.2	8.832
VDSL2 8c	G.994.2	8.5
VDSL2 8d	G.994.2	8.832
VDSL2 12a	G.994.2	12
VDSL2 12b	G.994.2	12
VDSL2 17a	G.994.2	17.664

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
VDSL2	8a	ITU G.994.2	8.32Mhz, / Power 17.5dBm; Max DS 50 Mbps
VDSL2	8b	ITU G.994.2	8.32Mhz, / Power 20.5dBm; Max DS 50 Mbps
VDSL2	8c	ITU G.994.2	8.5Mhz, / Power 11.5dBm; Max DS 50 Mbps
VDSL2	8d	ITU G.994.2	8.32Mhz, / Power 14.5dBm; Max DS 50 Mbps
VDSL2	12a	ITU G.994.2	12Mhz / Power 14.5 dBm; Max DS 68 Mbps
VDSL2	12b	ITU G.994.2	12Mhz / Power 14.5 dBm; Max DS 68 Mbps
VDSL2	17a	ITU G.994.2	17.664 Mhz / Power 14.5 dBm; Max DS 100 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	USO	ITU G.994.2	VDSL2 Upstream Band
Capability	G.Bond	ITU G.Bond	xDSL: Bandwidth aggregation of multiple lines
Capability	G.INP	ITU G.998.4	VDSL2: Protection for Severe Impulse Noise Interference
Capability	G.Vector	ITU G.993.5	VDSL2: Advance vector for minimizing cross-talk
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.
<input checked="" type="checkbox"/> G.Dmt Enabled	<input checked="" type="checkbox"/> 8a Enabled
<input checked="" type="checkbox"/> G.lite Enabled	<input checked="" type="checkbox"/> 8b Enabled
<input checked="" type="checkbox"/> T1.413 Enabled	<input checked="" type="checkbox"/> 8c Enabled
<input checked="" type="checkbox"/> ADSL2 Enabled	<input checked="" type="checkbox"/> 8d Enabled
<input checked="" type="checkbox"/> AnnexL Enabled	<input checked="" type="checkbox"/> 12a Enabled
<input checked="" type="checkbox"/> ADSL2+ Enabled	<input checked="" type="checkbox"/> 12b Enabled
<input checked="" type="checkbox"/> AnnexM Enabled	<input checked="" type="checkbox"/> 17a Enabled
<input checked="" type="checkbox"/> VDSL2 Enabled	

Capability	US0
<input checked="" type="checkbox"/> Bitswap Enable	<input checked="" type="checkbox"/> Enabled
<input checked="" type="checkbox"/> SRA Enable	

Phone Pair	xDSL Bonding
<input checked="" type="radio"/> Inner pair	<input checked="" type="checkbox"/> Enable DSL Bonding
<input type="radio"/> 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	<input type="checkbox"/>	Edit
ptm0.2	ipoe_4_1_1.200	IPoE	0	200	Enabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	Edit
ptm0.3	ipoe_4_1_1.10	IPoE	7	10	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

Add

Remove

WAN Interface Priority Schedule:

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

Apply/Save

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	
													Add	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: [0-255]

VCI: [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:

Service Category:

Minimum Cell Rate:

[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: [1-63]

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

VC WRR Weight: [1-63]

VC Precedence: [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.

Back

Apply/Save

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

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

http://192.168.5.1/ VisionNetGUI Welcome 'engineering' English

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

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

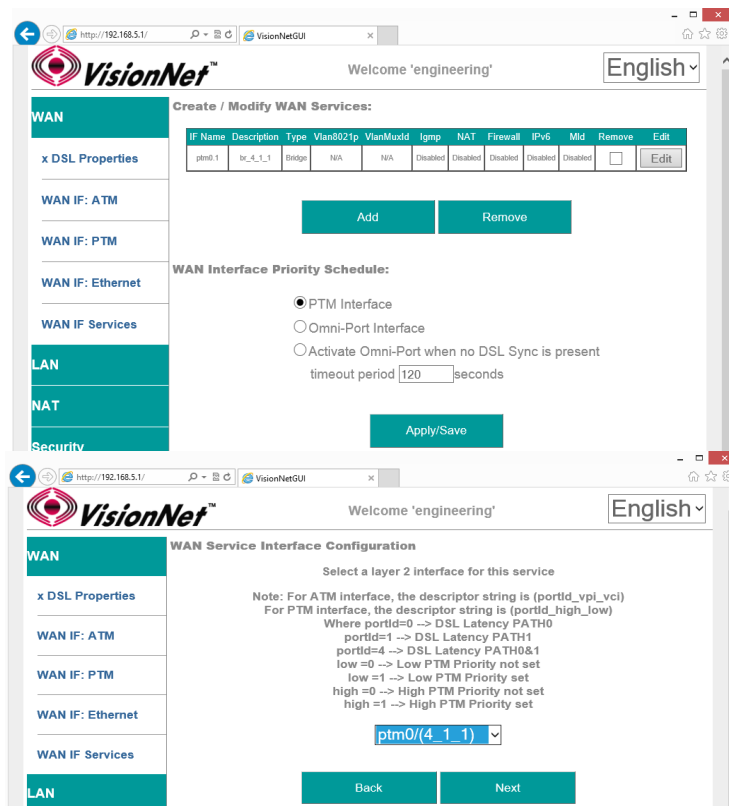
Notes:

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

- 2.B Select Desired Interface

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

Upon selection, select "Next"



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”

2.D WAN Summary

Upon Review, select “Apply/Save”

The first screenshot shows the 'WAN Service Configuration' page. The left sidebar has 'WAN' selected. The main area shows 'Select WAN service type:' with radio buttons for 'PPP over Ethernet (PPPoE)', 'IP over Ethernet', and 'Bridging' (selected). Below is an 'Enter Service Description:' field with 'br_4_1_1'. Further down are fields for 'Enter 802.1P Priority [0-7]:' and 'Enter 802.1Q VLAN ID [0-4094]:', both with '-1'. A 'Next' button is at the bottom right.

The second screenshot shows the 'WAN Setup - Summary' page. The left sidebar has 'WAN' selected. The main area shows a table of settings: Connection Type: Bridge, NAT: Disabled, Full Cone NAT: Disabled, Firewall: Disabled, IGMP Multicast: Not Applicable, and Quality Of Service: Disabled. Below the table is a note: 'Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.' 'Back' and 'Apply/Save' buttons are at the bottom.

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”

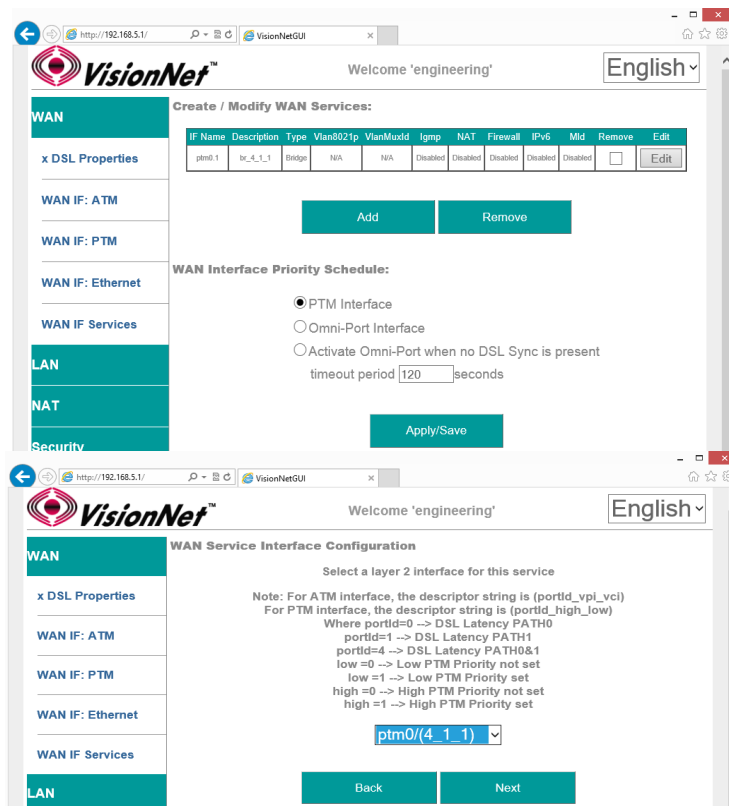
Notes:

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

- 2.B Select Desired Interface

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

Upon selection, select “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”

The screenshot shows the 'WAN Service Configuration' page in the VisionNet GUI. The left sidebar has 'WAN' selected. The main content area includes: 'Select WAN service type:' with radio buttons for 'PPP over Ethernet (PPPoE)', 'IP over Ethernet' (selected), and 'Bridging'; 'Enter Service Description:' with a text box containing 'ipoe_4_0_35'; 'Enter 802.1P Priority [0-7]:' with a text box containing '7'; 'Enter 802.1Q VLAN ID [0-4094]:' with a text box containing '201'; 'Network Protocol Selection:' with a dropdown menu set to 'IPv4&IPv6(Dual Stack)'; and 'Back' and 'Next' buttons at the bottom.

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”

The screenshot shows the 'WAN IP Settings' page in the VisionNet GUI. The left sidebar has 'WAN' selected. The main content area includes: 'Enter information provided to you by your ISP to configure the WAN IP settings.' with a notice about DHCP; 'Obtain an IP address automatically' with radio buttons for 'Option 60 Vendor ID', 'Option 61 IAID', 'Option 61 DUID', and 'Option 125'; 'Use the following Static IP address:' with text boxes for 'WAN IP Address', 'WAN Subnet Mask', and 'WAN gateway IP Address'; 'Enter information provided to you by your ISP to configure the WAN IPv6 settings.' with a notice about DHCPv6; 'Obtain an IPv6 address automatically' with radio buttons for 'Dhcpv6 Address Assignment (IANA)', 'Dhcpv6 Prefix Delegation (IAPD)', and 'Use the following Static IPv6 address:'; 'WAN IP v6 Address/Prefix Length:' with a text box; and 'Specify the Next-Hop IPv6 address for this WAN interface.' with a text box for 'WAN Next-Hop IPv6 Address:'. 'Back' and 'Next' buttons are at the bottom.

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

The screenshot shows the 'Network Address Translation Settings' page in the VisionNet GUI. The left sidebar has 'WAN' selected. The main content area includes: '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' (checked) and 'Enable Fullcone NAT' (unchecked); 'Enable Firewall' (checked); 'IGMP Multicast' section with 'Enable IGMP Multicast' (unchecked), 'No Multicast VLAN Filter' (unchecked), and 'Enable MLD Multicast Proxy' (unchecked); and 'Back' and 'Next' buttons at the bottom.

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.

2.G Add Service to DNS Priority List

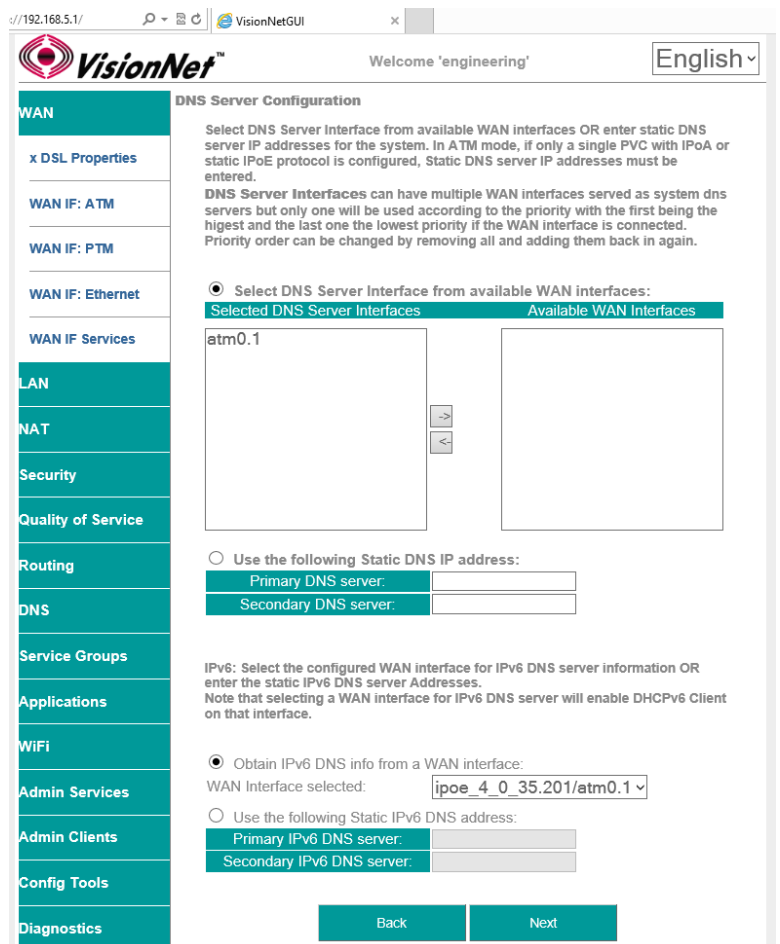
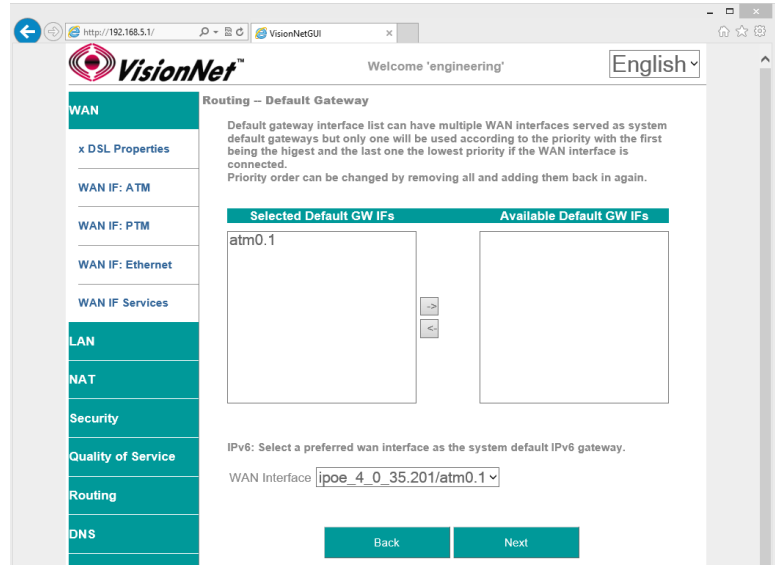
(Not available in WAN Modification; For post creation Modification See Section X)

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.



2.H WAN Summary

Upon Review, select “Apply/Save”

ip://192.168.5.1/ VisionNetGUI x

VisionNet™ Welcome 'engineering' English ▾

WAN

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

WAN Setup - Summary

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

Connection Type:	PoE
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.

Back Apply/Save

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:

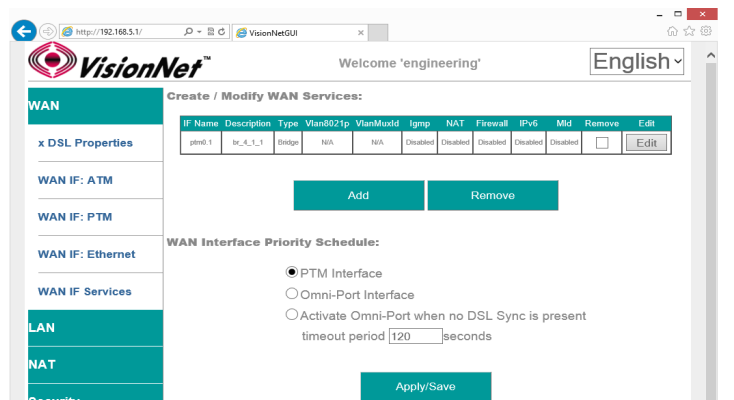
WAN

WAN IF: Services

Step 2 Create a WAN Interface

- 2.A Select “Add”

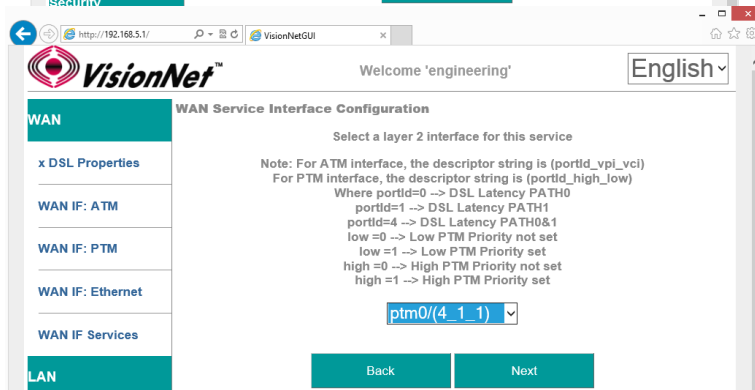
NOTE: If you wish to modify an existing connection; select the “EDIT” button located in the table row of the desired interface



- 2.B Select Desired Interface

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

Upon selection, select “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”

The screenshot shows the VisionNet GUI for WAN Service Configuration. The browser address bar shows //192.168.5.1/. The page title is 'VisionNet' and the user is logged in as 'engineering'. The language is set to English. The left sidebar contains navigation tabs: WAN (selected), DSL Properties, ATM, PTM, Ethernet, WAN IF Services, LAN, NAT, Security, and Quality of Service. The main content area is titled 'WAN Service Configuration' and includes the following sections:

- Select WAN service type:** Three radio buttons are present: 'PPP over Ethernet (PPPoE)' (selected), 'IP over Ethernet', and 'Bridging'.
- Enter Service Description:** A text input field containing '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]:** A text input field containing '-1'.
- Enter 802.1Q VLAN ID [0-4094]:** A text input field containing '-1'.
- Network Protocol Selection:** A dropdown menu with 'IPv4&IPv6(Dual Stack)' selected.
- Buttons:** 'Back' and 'Next' buttons are located at the bottom right of the configuration area.

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”

The screenshot shows the VisionNet configuration interface. The top navigation bar includes the VisionNet logo, a welcome message for 'engineering', and a language dropdown set to 'English'. The main content area is titled 'PPP Username and Password' and contains a text box with instructions: '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.' Below this are input fields for 'PPP Username' (containing 'username'), 'PPP Password' (masked with dots), 'PPPoE Service Name' (empty), and 'Authentication Method' (set to 'AUTO'). A list of checkboxes follows: 'Enable NAT' (checked), 'Enable Fullcone NAT' (unchecked), 'Enable Firewall' (checked), 'Dial on demand (with idle timeout timer)' (checked), and 'Inactivity Timeout (minutes) [1-4320]:' (set to '0'). Further down, there are checkboxes for 'PPP IP extension', 'Use Static IPv4 Address', 'Use Static IPv6 Address', 'Enable IPv6 Unnumbered Model', 'Launch Dhcp6c for Address Assignment (IANA)' (checked), 'Launch Dhcp6c for Prefix Delegation (IAPD)' (checked), 'Enable PPP Debug Mode' (checked), and 'Bridge PPPoE Frames Between WAN and Local Ports' (checked). At the bottom, there are checkboxes for 'Multicast Proxy' options: 'Enable IGMP Multicast Proxy' (unchecked) and 'Enable MLD Multicast Proxy' (unchecked). 'Back' and 'Next' buttons are located at the bottom right of the configuration area.

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.

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.

2.G WAN Summary

Upon Review, select “Apply/Save”

The screenshot shows the 'Routing - Default Gateway' configuration page in the VisionNet web interface. The left sidebar contains a navigation menu with 'WAN' selected. The main content area has a header 'Welcome 'engineering'' and a language dropdown set to 'English'. Below the header, there is a description: '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 highest 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.' There are two columns: 'Selected Default GW IFs' containing 'atm0.1' and 'Available Default GW IFs' containing 'ppp0.1'. Below these columns are navigation arrows. At the bottom, there is a section for IPv6 configuration: 'IPv6: Select a preferred wan interface as the system default IPv6 gateway.' with a dropdown menu showing 'ipoe_4_0_35.201/atm0.1' and 'Back' and 'Next' buttons.

The screenshot shows the 'DNS Server Configuration' page in the VisionNet web interface. The left sidebar contains a navigation menu with 'WAN' selected. The main content area has a header 'Welcome 'engineering'' and a language dropdown set to 'English'. Below the header, there is a description: '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 highest 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.' There are two columns: 'Selected DNS Server Interfaces' containing 'atm0.1' and 'ppp0.1', and 'Available WAN Interfaces' which is empty. Below these columns are navigation arrows. There are two radio button options: 'Select DNS Server Interface from available WAN interfaces:' (selected) and 'Use the following Static DNS IP address:'. The static option has input fields for 'Primary DNS server:' and 'Secondary DNS server:'. Below that, there is a section for IPv6: '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.' There are two radio button options: 'Obtain IPv6 DNS info from a WAN interface:' (selected) and 'Use the following Static IPv6 DNS address:'. The static option has input fields for 'Primary IPv6 DNS server:' and 'Secondary IPv6 DNS server:'. At the bottom, there are 'Back' and 'Next' buttons.

The screenshot shows the 'WAN Setup - Summary' page in the VisionNet web interface. The left sidebar contains a navigation menu with 'WAN' selected. The main content area has a header 'Welcome 'engineering'' and a language dropdown set to 'English'. Below the header, there is a description: 'Make sure that the settings below match the settings provided by your ISP.' There is a table with two columns: 'Connection Type:' and 'Status:'. The rows are: 'NAT: Checked', 'Full Cone NAT: Checked', 'Firewall: Checked', 'IGMP Multicast: Checked', and 'Quality Of Service: Checked'. Below the table, there is a note: 'Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.' At the bottom, there are 'Back' and 'Apply/Save' buttons.

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

The screenshot shows the VisionNet web interface. At the top, there is a logo for VisionNet and a welcome message for the user 'engineering'. A language dropdown menu is set to 'English'. The main content area is titled 'Universal Quality of Service Enablement'. On the left, there is a navigation menu with options: WAN, LAN, NAT, Security, and Quality of Service (which is highlighted). The main content area contains a checkbox labeled 'Enable QoS' which is checked. Below it, there is a label 'Select Default DSCP Mark' followed by a dropdown menu currently showing 'No Change(-1)'. At the bottom right of the form, there is a teal button labeled 'Apply/Save'.

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.

- 2.B When finished, select “ **Apply / Save** ”.

WAN

LAN

NAT

Security

Quality of Service

Enable QoS

QoS Queue

Egress Class Rules

Routing

DNS

Service Groups

Applications

WiFi

Admin Services

QoS Queue Table

QoS Dependent upon QoS Enablement

WMM (WiFi) QoS Dependent upon WMM Enablement

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	wi0	8	1/SP						Enabled	
WMM Voice Priority	2	wi0	7	2/SP						Enabled	
WMM Video Priority	3	wi0	6	3/SP						Enabled	
WMM Video Priority	4	wi0	5	4/SP						Enabled	
WMM Best Effort	5	wi0	4	5/SP						Enabled	
WMM Background	6	wi0	3	6/SP						Enabled	
WMM Background	7	wi0	2	7/SP						Enabled	
WMM Best Effort	8	wi0	1	8/SP						Enabled	
Default Queue	33	atm0	1	8/WFQ/1	Path0					<input checked="" type="checkbox"/>	
Default Queue	34	atm1	1	1/WFQ/1	Path0					<input checked="" type="checkbox"/>	
Default Queue	35	ptm0	1	1/WFQ/1	Path0	Low				<input checked="" type="checkbox"/>	
Default Queue	36	atm2	1	8/WFQ/1	Path0					<input checked="" type="checkbox"/>	

Add
Enable
Remove

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

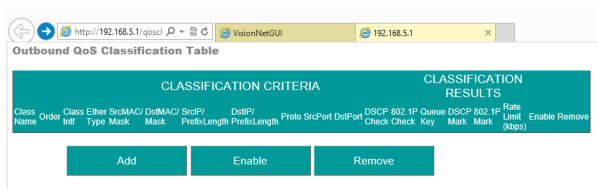
Egress Class Rules

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”



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”

- 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

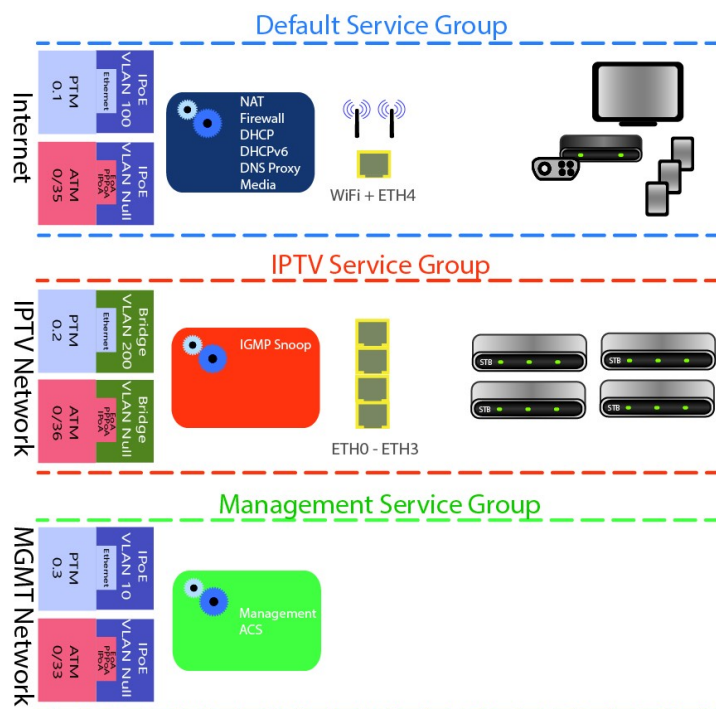
2.A WAN Services are grouped by service type.

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

Service Groups

[IF / Service Groups](#)

Applications

WiFi

Admin Services

Admin Clients

Config Tools

Diagnostics

Statistics

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:

Grouped Interfaces	Available Interfaces
atm1.1	atm0.1
ptm0.2	atm2.1
Ethernet 1	ptm0.1
Ethernet 2	ptm0.3
Ethernet 3	Omni Port
Ethernet 4	wlan0

Automatically Add Clients With the following DHCP Vendor IDs

Apply/Save

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	<input type="checkbox"/>	atm0.1 atm2.1 ptm0.1 ptm0.3	wlan0 Omni Port	
IPTV	<input type="checkbox"/>	atm1.1 ptm0.2	Ethernet 1 Ethernet 2 Ethernet 3 Ethernet 4	

Add **Remove**

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:



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.

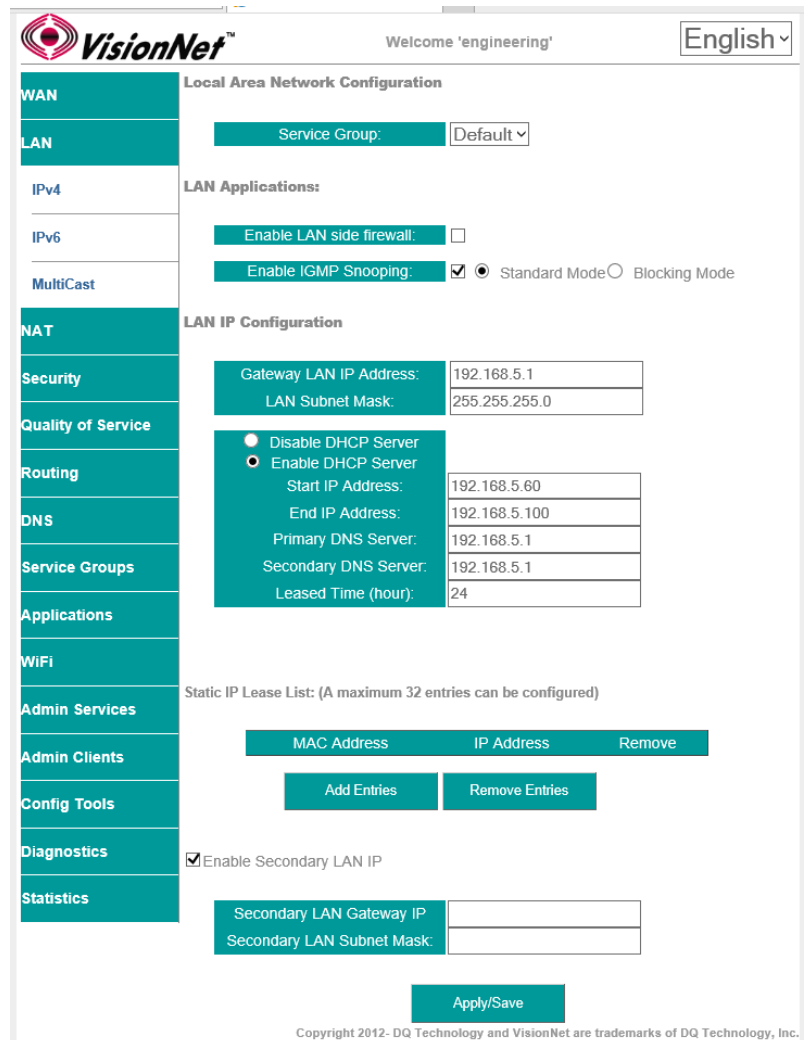
DNS Proxy may be by-passed (WAN DNS will be passed to devices). See Section 4.X

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



The screenshot shows the VisionNet web interface for 'Local Area Network Configuration'. The left sidebar contains a navigation menu with options: WAN, LAN (selected), IPv4, IPv6, MultiCast, NAT, Security, Quality of Service, Routing, DNS, Service Groups, Applications, WiFi, Admin Services, Admin Clients, Config Tools, Diagnostics, and Statistics. The main content area is titled 'Local Area Network Configuration' and includes a 'Service Group' dropdown set to 'Default'. Under 'LAN Applications', there are checkboxes for 'Enable LAN side firewall' (unchecked) and 'Enable IGMP Snooping' (checked), with radio buttons for 'Standard Mode' (selected) and 'Blocking Mode'. The 'LAN IP Configuration' section includes fields for 'Gateway LAN IP Address' (192.168.5.1) and 'LAN Subnet Mask' (255.255.255.0). Below this, there are radio buttons for 'Disable DHCP Server' (selected) and 'Enable DHCP Server'. The 'Enable DHCP Server' section has fields for '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), and 'Leased Time (hour)' (24). A 'Static IP Lease List' section is present with a table header for 'MAC Address', 'IP Address', and 'Remove', and buttons for 'Add Entries' and 'Remove Entries'. There is a checkbox for 'Enable Secondary LAN IP' which is checked. Below it are fields for 'Secondary LAN Gateway IP' and 'Secondary LAN Subnet Mask'. An 'Apply/Save' button is at the bottom. A copyright notice at the bottom right reads: '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:



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

Step 3 When finished, select “ [Apply / Save](#) “.

LAN
MultiCast

English

Welcome 'engineering'

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:	<input checked="" type="checkbox"/>
LAN to LAN (Intra LAN) Multicast Enable:	<input type="checkbox"/>
Membership Join Immediate (IPTV):	<input type="checkbox"/>

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.

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

The screenshot shows the VisionNet web interface for configuring gateway priorities. The left navigation pane includes WAN, LAN, NAT, Security, Quality of Service, Routing, IF Default Gateway, IP Tunnel 6 in 4, IP Tunnel 4 in 6, Static Route Table, and Policy Route Table. The 'Routing' section is active, showing the 'Interface Gateway Priority' configuration. The page title is 'Interface Gateway Priority' and the user is logged in as 'engineering'. The interface is in English. The configuration area is divided into two columns: 'Selected Default GW IFs' and 'Available Default GW IFs'. The 'Selected' column contains 'atm0.1' and 'ptm0.1'. The 'Available' column contains 'atm2.1' and 'ptm0.3'. Below the columns are controls for 'Select Default IPv6 Gateway' and a 'WAN Interface' dropdown set to 'ipoe_4_1_1.100/ptm0.1'. An 'Apply/Save' button is at the bottom right.

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
------------	---------------------	---------	-----------	--------	--------

Add 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

Apply/Save

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"**

The screenshot shows the VisionNet web interface. At the top, there is a logo and a welcome message 'Welcome 'engineering''. Below this, a navigation menu includes 'WAN', 'LAN', and 'NAT'. The main content area is titled 'Host Policy Route Table -- A maximum 7 entries can be configured.' It features a table with columns: Policy Name, Source IP, LAN Port, WAN, Default GW, and Remove. Below the table are two buttons: 'Add' and '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 if 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

The screenshot shows the 'Add Policy Route' form in the VisionNet web interface. It includes a navigation menu with 'WAN', 'LAN', 'NAT', 'Security', 'Quality of Service', 'Routing', 'IP Default Gateway', 'IP Tunnel 6 in 4', 'IP Tunnel 4 in 6', and 'Static Route Table'. The form fields are: Policy Name (NewPolicy), Physical LAN Port (dropdown), Source IP (192.168.5.1), Use Interface (ipoe_eth4/eth4.1), and Default Gateway IP (172.20.20.1). An 'Apply/Save' button is at the bottom.

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 ptm0.1	atm2.1 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:

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 assigned IPv4 DNS Servers”.

IPv4

Enter Primary and Secondary

VisionNet™ Welcome 'engineering' English ▾

DNS Server Configuration

IPv4 DNS:

Select WAN Interface for Default IPv4 DNS Source:

Selected DNS Server Interfaces	Available WAN Interfaces
atm0.1 ptm0.1	atm2.1 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:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Apply/Save

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 surveillance 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:

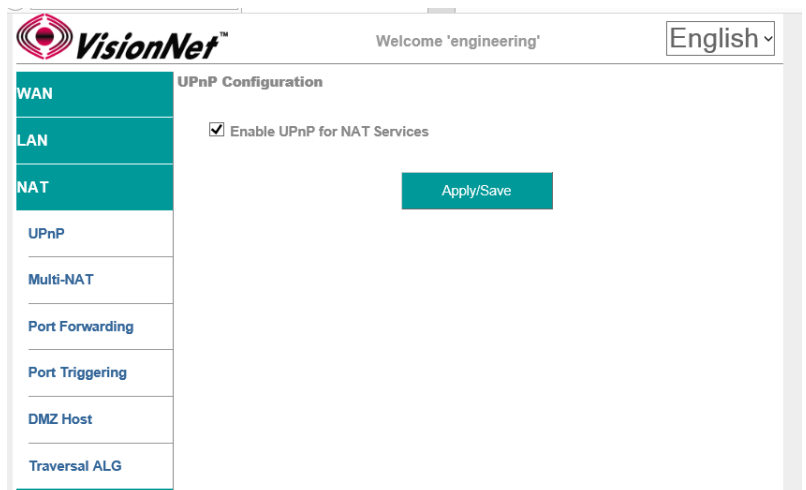


Step 2 Enable / Disable UPnP

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

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

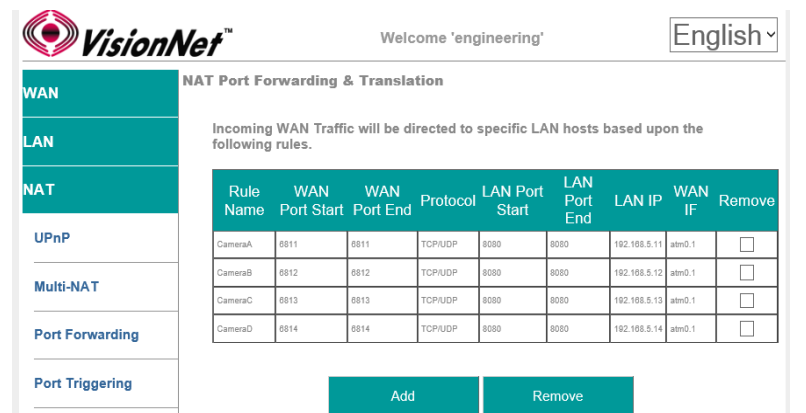
For this reason, non-standard management ports are always suggested.



2.B



Port Forwarding



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

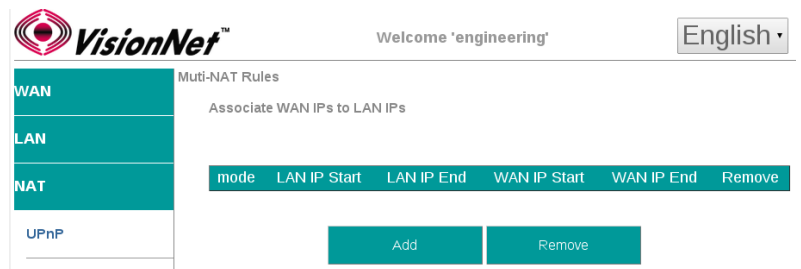
Step 1 Direct your browser to the **Multi-NAT** page

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



Step 2 Create Multi-NAT Rules

2.A Select “Add”



2.B Rule Type

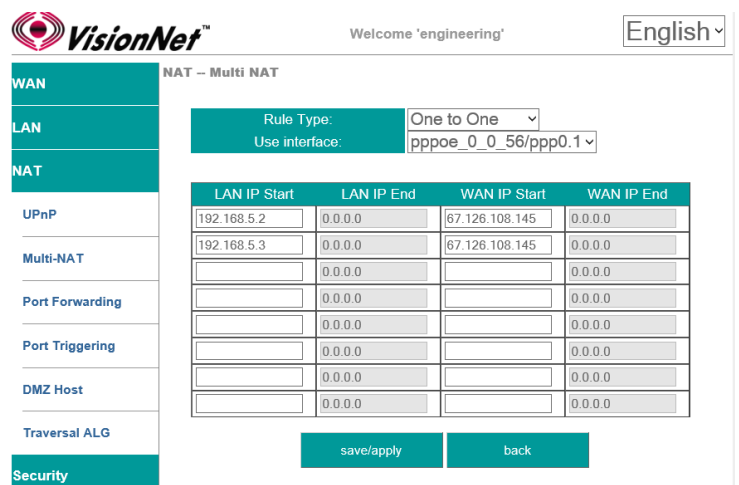
- 1:1 : 1 LAN IP ↔ 1 WAN IP
- 1: Many : 1 LAN IP ↔ >1 WAN IP
- Many:1: >1 LAN IP ↔ 1 WAN IP
- Many: Many : >1 LAN IP ↔ >1 WAN IP

Use Interface

WAN interface associated with the rule

IP Ranges

Associated with Rule Types



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

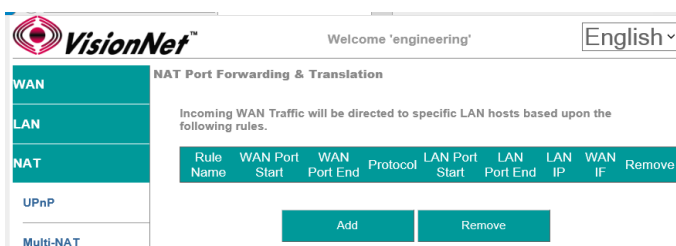
- 1.A In the left-hand navigation pane, select:

NAT

Port Forwarding

Step 2 Create Port Forwarding Rules

- 2.A Select “Add”



- 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

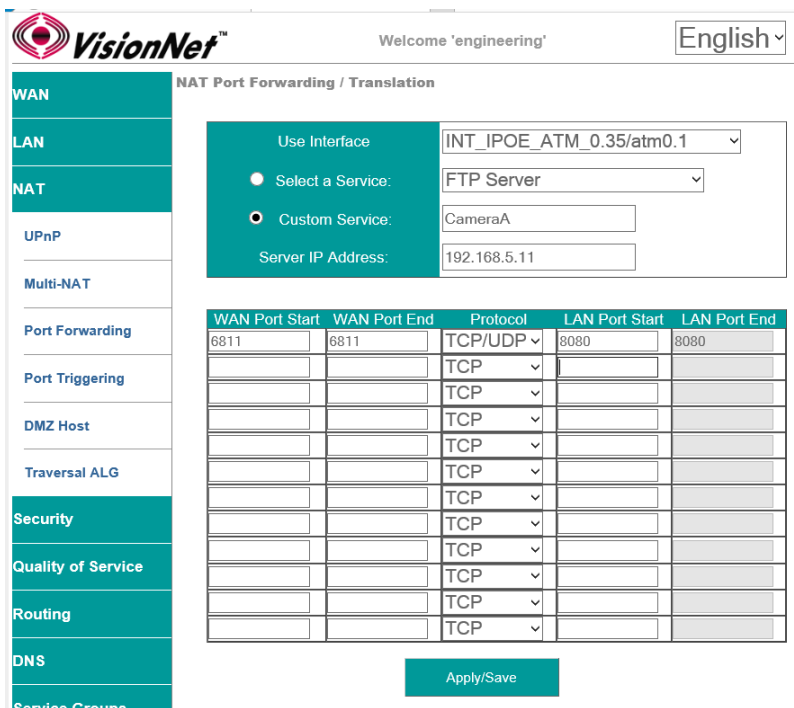
First and Last ports in entry (ie:6900)

Protocol

TCP, UDP, or TCP/UDP

LAN Port Start / End

First and Last ports in entry (ie:6900)



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”

VISIONNet™ Welcome 'engineering' English

NAT Port Triggering

Dynamic Port Forwarding rules will be activated by LAN host activity

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

Add Remove

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

VISIONNet™ Welcome 'engineering' English

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

Save/Apply

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

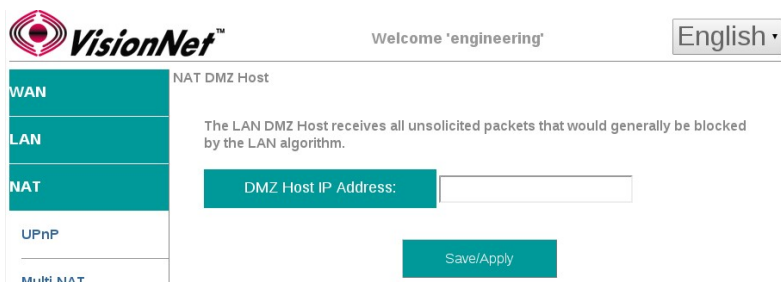
- 1.A In the left-hand navigation pane, select:

NAT

DMZ Host

Step 2 Specify DMZ Host

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



The screenshot shows the VisionNet web interface. At the top left is the VisionNet logo. To the right, it says "Welcome 'engineering'" and "English". A navigation menu on the left lists WAN, LAN, NAT, UPnP, and MultiNAT. The NAT menu item is highlighted. The main content area is titled "NAT DMZ Host" and contains the text: "The LAN DMZ Host receives all unsolicited packets that would generally be blocked by the LAN algorithm." Below this text is a form with a label "DMZ Host IP Address:" and an empty input field. A "Save/Apply" button is located below the input field.

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 accommodate 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

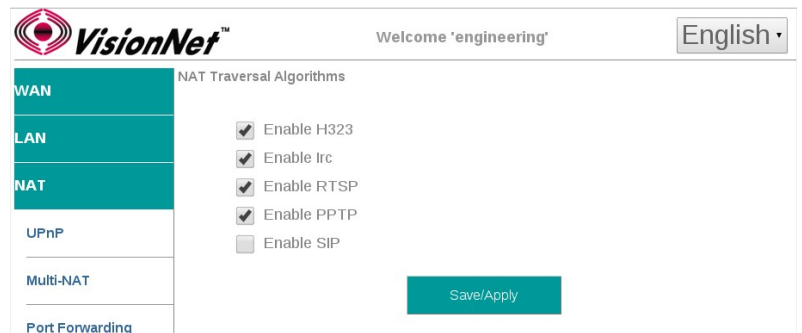
1.A In the left-hand navigation pane, select:

NAT

Traversal ALG

Step 2 Enable / Disable requested ALG

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



The screenshot shows the VisionNet web interface for configuring NAT Traversal Algorithms. The page title is "NAT Traversal Algorithms" and the user is logged in as "engineering". The left navigation pane has "NAT" selected. The main content area shows a list of algorithms with checkboxes: "Enable H323" (checked), "Enable Irc" (checked), "Enable RTSP" (checked), "Enable PPTP" (checked), and "Enable SIP" (unchecked). A "Save/Apply" button is located at the bottom right of the configuration area.

Step 3 When finished, select “ [Apply / Save](#) “.

SECTION 9: WiFi Configuration

SECTION 9.1 Enable / Disable WiFi

Abstract:

WiFi may be enabled / disabled

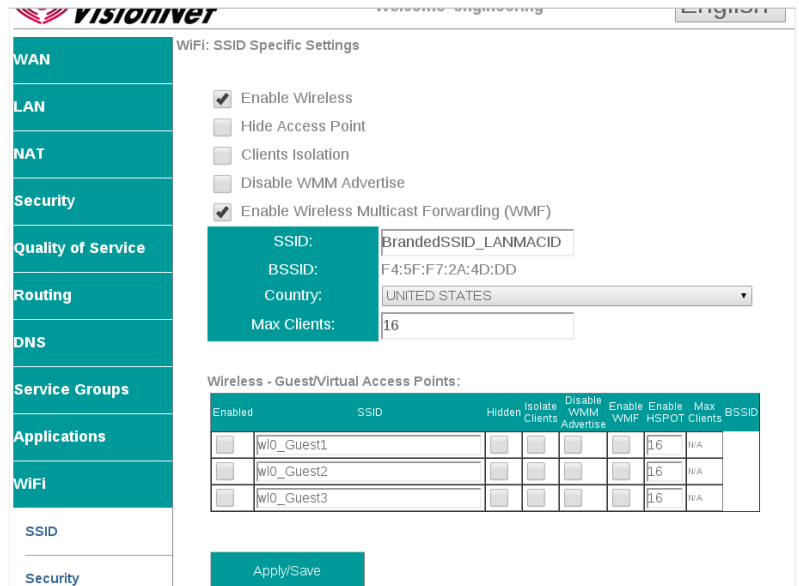
Step 1 Direct your browser to the **SSID** page

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



Step 2 Enable / Disable WiFi

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



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

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

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

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

The screenshot shows the VisionNet M625N R1 configuration interface. The left sidebar contains a navigation menu with the following items: WAN, LAN, NAT, Security, Quality of Service, Routing, DNS, Service Groups, Applications, WiFi, SSID, and Security. The main content area is titled "WiFi: SSID Specific Settings" and includes the following options:

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

Below these options are input fields for:

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

At the bottom, there is a table titled "Wireless - Guest/Virtual Access Points:" with the following columns: Enabled, SSID, Hidden, Isolate Clients, Disable WMM Advertise, Enable WMF, Enable HSPOT, Max Clients, and BSSID.

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Enable HSPOT	Max Clients	BSSID
<input type="checkbox"/>	Wl0_Guest1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A
<input type="checkbox"/>	Wl0_Guest2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A
<input type="checkbox"/>	Wl0_Guest3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A

At the bottom of the page, there is an "Apply/Save" button.

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:



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

A screenshot of the VisionNet web interface. The top left shows the VisionNet logo. The top right says "Welcome 'engineering'" and "English". A left-hand navigation pane has "WiFi" selected. The main content area is titled "WiFi: Security". It shows "WPS is disabled by default" and "Manual Configuration is suggested". Under "WPS Setup", there is a teal "Enable WPS" button and a "Disabled" dropdown. Under "Manual Configuration", there is a "Select SSID:" dropdown set to "BrandedSSID_LANMACID", a "Network Authentication:" dropdown set to "WPA2 -PSK", a "WPA/WAPI passphrase:" text field with a "Click here to display" link, a "WPA Group Rekey Interval:" text field set to "0", a "WPA/WAPI Encryption:" dropdown set to "AES", and a "WEP Encryption:" dropdown set to "Disabled". At the bottom right is an "Apply/Save" button.

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:



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 Advertisement 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 Interval 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

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
- G.Bond (ADSL2+/VDSL2)
- ADSL2 / ADSL2+
- VDSL2 (8a,b,c,d/12a,b/17a)
- SRA
- Bitswap
- G.Vector
- 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

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

Management Protocols

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

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

Diagnostic Features

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

Hardware Specifications

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

LAN: Switch A: 1 Port Gbe

LAN Switch B: 1 Port Gbe, 3 Port 10/100 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)

WAN Service Features

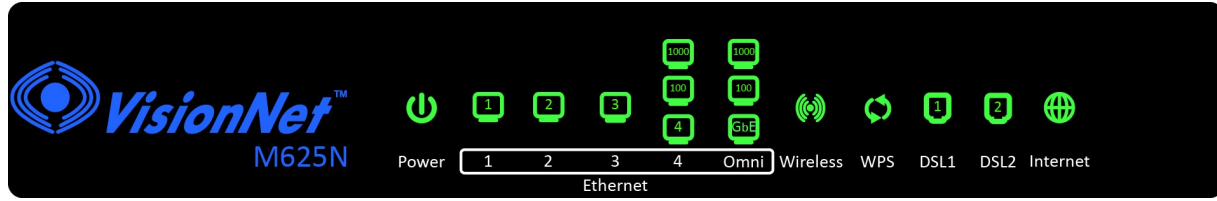
- Bridge
- IPoE
- VLAN MUX / Tagging
- IPv4, IPv6
- PPPoE (PAP,CHAP,Auto) • IGMP Proxy/Multi-cast
- PPPoA
- PPP IP Extension
- IPoA
- ATM QoS, FWQ, MPAAL
- Group Specific Routing • ATM Priority Queing
- Multi-Protocol Encapsulation
- Multiple Services Connection
- Multi-Option DHCP

Wi Fi Features

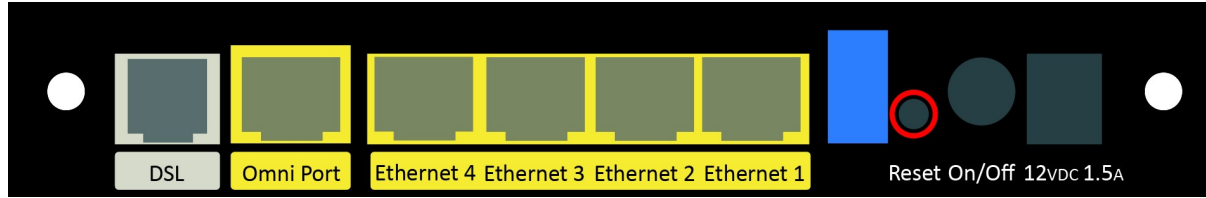
- 802.11b/g/n 2T2R
- 2.4Ghz 20/40Mhz
- 17dBm
- Qty 2 -3 dbi RP-SMA
- WEP, WPA, WPA2, PSK
- AES, TKIP
- 802.1x Radius Support
- WPS
- 1 Main, 3 Guest SSIDs
- WMM, WAPSD, QoS
- UMA Mobile Converge

SECTION 10.2 Product Depictions

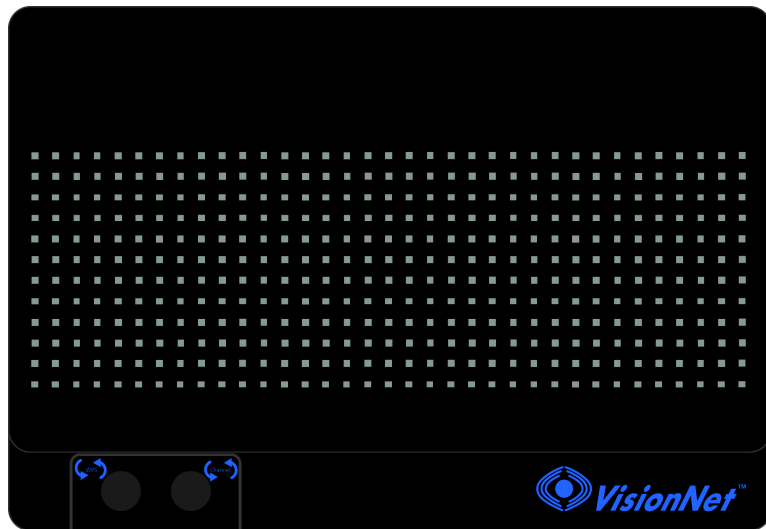
Front Depiction



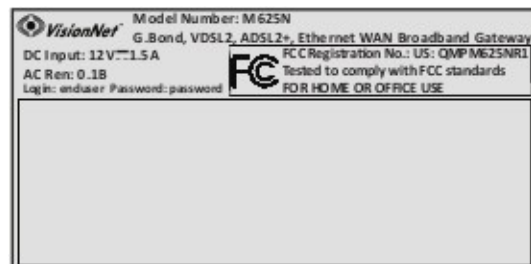
Back Depiction



Top Depiction



Label Depiction



SECTION 10.3 LED Functionality

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

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: M625N

FCC ID: QMPM625NR1

US: DQ1DL01BM625NR1

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 cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

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

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: DQ1DL01BM625NR1] 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: DQ1DL01BM625NR1], 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: DQ1DL01BM625NR1]

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: DQ1DL01BM625NR1] indicates the REN would be. 0.1.

SECTION 10.5 FIRMWARE RELEASE NOTES

Firmware Build Timestamp: 131223

Updates/Changes

1. DNS

Updated DNS Algorithm regarding AAAA DNS queries

Firmware Build Timestamp: 131210

Updates/Changes

1. G.Vectoring

G.Vectoring Protocol enabled by Default

2. DSL Phy Driver Change

DSL Phy Revision updated to: A2pvbF039g1.d24n

Firmware Build Timestamp: 131127

Updates/Changes

1. DNS Proxy

Resolve issue with rare cases of DNS Proxy process crashing

Firmware Build Timestamp: 131022

Updates/Changes

1. DNS

Added Support for Static DNS
Option is located under DNS -> DNS Proxy

2. DHCP Options

Added Support for:
DHCP Option 2 and 42: Network Time Protocol
DHCP Option 43: ACS URL
DHCP Option 66: TFTP URL for LAN Clients

3. QoS Classification

4. Multicast Precedence

Support Multiple WAN Connections for same QoS Classification Rules
Removed from GUI

5. GUI Optimization

Updated GUI Scrolling Behavior

6. TCP Throughput tools

Added TTCP support for throughput testing

7. Server Timeout Function

Added support for timeout function for Admin Services