Product Manual

Model: M405 R3

Product Description: Broadband Gateway

WAN: ADSL2+
Ethernet: Qty 1- 10/100 Ethernet
USB: 1.1 (Management)
# 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  
1.6 USB MANAGEMENT 11

## SECTION 2: WAN CONFIGURATION

2.1 WAN LOGIC OVERVIEW 12  
2.2 X DSL LOGIC 14  
2.3 CUSTOMIZING X DSL PARAMETERS 16  
2.4 CREATING AN ATM INTERFACE 17  
2.5 CREATE/MODIFY A BRIDGED WAN SERVICE 18  
2.6 CREATE/MODIFY AN IPOE WAN SERVICE 20  
2.7 CREATE/MODIFY A PPP WAN SERVICE 23

## SECTION 3: QUALITY OF SERVICE

3.1 QUALITY OF SERVICE ENABLE/DISABLE 26  
3.2 INTERFACE CONFIGURATION 27  
3.3 QOS CLASSIFICATION TABLE 28

## SECTION 4: SERVICE GROUPS

4.1 SERVICE GROUP LOGIC 29  
4.2 SERVICE GROUP CREATION 29

## SECTION 5: IPv4 LAN CONFIGURATION

5.1 IPv4 CONFIGURATION 31  
5.2 IGMP MULTICAST 32

## SECTION 6: IPv4 ROUTE CONFIGURATION

6.1 GATEWAY PRIORITIZATION 33  
6.2 STATIC ROUTE TABLE 34
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 overwritten 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:

<table>
<thead>
<tr>
<th>Access</th>
<th>Account Name</th>
<th>GUI Privilege</th>
<th>CLI Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>engineering</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Local</td>
<td>technician</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Local</td>
<td>enduser</td>
<td>Low</td>
<td>None</td>
</tr>
<tr>
<td>Remote</td>
<td>networkops</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Remote</td>
<td>techsupport</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Service</th>
<th>LAN Port / Status</th>
<th>WAN Port - Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80 - Enabled</td>
<td>6080 - Enabled</td>
</tr>
<tr>
<td>TELNET</td>
<td>23 - Enabled</td>
<td>6023 - Disabled</td>
</tr>
<tr>
<td>SSH</td>
<td>22 - Enabled</td>
<td>6022 - Enabled</td>
</tr>
<tr>
<td>FTP</td>
<td>21 - Disabled</td>
<td>21 - Disabled</td>
</tr>
<tr>
<td>TFTP</td>
<td>69 - Enabled</td>
<td>69 - Disabled</td>
</tr>
<tr>
<td>ICMP</td>
<td>N/A - Enabled</td>
<td>N/A - Enabled</td>
</tr>
<tr>
<td>SNMP</td>
<td>161 - Disabled</td>
<td>161 - Disabled</td>
</tr>
<tr>
<td>SAMBA</td>
<td>445 - Enabled</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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 1.6 USB Management

**STEP 1  Understanding the USB Management Function**

1.A The USB 1.1 Port, on the M405R3, is designed to operate as a standard Ethernet Adapter.

As of March 2014, the USB Adapter has been tested with

- MAC OSX
- Windows 7
- Fedora Linux 21
- Ubuntu Linux 13.10

without the need for custom drivers. No warranty regarding long term driver support for any specific OS is provided or implied.

In the event that a device is not isolated to a management service group, it will be able to route as a traditional ethernet connect.

This is a particularly useful function for Port Mirroring of Bridge applications.

**Step 2  Connect via Client**

2.A Your documentation will determine whether your USB device is isolated from the general LAN.

In the event that you have DHCP disabled for your isolated LAN Group, or you have DHCP disabled due to a bridged WAN application, you will need to statically assign a local IP to manage your device.

Even if your device is bridged, there is still a LAN interface, with a local IP, accessible to you.
SECTION 2: WAN CONFIGURATION

SECTION 2.1  WAN LOGIC OVERVIEW

1. A  WAN IF (Interfaces)

The M405 supports ATM “Layer 1 – 2” WAN Configurations

ATM
Available for: xDSL Interface
Most Commonly Associated with ADSL

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
2.A Building WAN Services

WAN Services Must be added as follows:

1: Add & Define WAN Interface
   ATM

2: Add and Define Service to Interface
   ATM

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
SECTION 2.2  x DSL LOGIC

**Item 1  x DSL Physical Interfaces**

1.A  xDSL Port Layout

   **Line Pinout**

   The M405 supports inner pair operation only

1.B  xDSL Line Cord Preferences

   DSL line cords should not create unnecessary attenuation or cross-talk.

2.B  ADSL2+ Associations

   **ADSL – ADSL2+**

   - **Operating Frequency:**
     20 KHz – 2.2 Mhz

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

   - **General Operation:**
     ATM

<table>
<thead>
<tr>
<th>Standard</th>
<th>ITU Standard</th>
<th>Max Frequency (Mhz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL</td>
<td>G.992.1</td>
<td>1.1</td>
</tr>
<tr>
<td>ADSL2</td>
<td>G.992.3</td>
<td>1.1</td>
</tr>
<tr>
<td>ADSL2+</td>
<td>G.992.5</td>
<td>2.2</td>
</tr>
</tbody>
</table>
Below, is a brief summary of some xDSL protocols to familiarize yourself with:

<table>
<thead>
<tr>
<th>Class</th>
<th>Protocol</th>
<th>Standard</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL</td>
<td>G.DMT</td>
<td>ITU G.992.1</td>
<td>8Mbps DS / 1.3 Mbps US</td>
</tr>
<tr>
<td>ADSL</td>
<td>G.Lite</td>
<td>ITU G.992.2</td>
<td>1.5 Mbps DS / 512 kbps US</td>
</tr>
<tr>
<td>ADSL</td>
<td>T1.413</td>
<td>ANSI T1.413</td>
<td>8Mbps DS / 1.3 Mbps US</td>
</tr>
<tr>
<td>ADSL2</td>
<td>ADSL</td>
<td>ITU G.992.3</td>
<td>12 Mbps DS / 800 kbps US</td>
</tr>
<tr>
<td>ADSL2</td>
<td>Annex L</td>
<td>ITU G.992.3</td>
<td>Increases ADSL2 Reach to 7 km (23k ft)</td>
</tr>
<tr>
<td>ADSL2+</td>
<td>ADSL2+</td>
<td>ITU G.992.5</td>
<td>Doubles Frequency Range from 1.1Mhz to 2.2 Mhz</td>
</tr>
<tr>
<td>ADSL2+</td>
<td>Annex M</td>
<td>ITU G.992.5</td>
<td>Changes DS / US frequency split, to double US to max 3.3 Mbps</td>
</tr>
<tr>
<td>Capability</td>
<td>Bitswap</td>
<td>ITU G.992.1</td>
<td>Allows for movement of bit transmission between “bins”</td>
</tr>
<tr>
<td>Capability</td>
<td>SRA</td>
<td>ITU G.992.5</td>
<td>ADSL2+: Allows for rate changes without re-training</td>
</tr>
<tr>
<td>Capability</td>
<td>PhyR</td>
<td>Proprietary</td>
<td>ADSL2+: Physical Layer ReTransmission - Broadcom support only</td>
</tr>
</tbody>
</table>
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 ISP’s 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:

![xDLS 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.

2.B Select “Save / Apply”
SECTION 2.4 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:

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.

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 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

Service Connection Type
Default does not allow for VLANs, and only one connection per PVC. VLAN Mux allows for multiple VLANs over a single PVC.
MSC Mode allows for multiple untagged connection over a signle PVC.

Encapsulation Mode
Default: LLC/Snap-Bridging

Service Category
Default: UBR without PCR

QoS Scheduler
Enabling IP QoS will allow you to prioritize upstream packets between multiple connections. This will generally remain unused for single port units.

2.C Select “Apply / Save”
SECTION 2.5 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 IF: Services](image)

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)

   If you did not wish to use tagged connections, you must re-build the ATM connection as Default mode

   Once complete, select “Next”
2.D  WAN Summary

Upon Review, select "Apply/Save"

<table>
<thead>
<tr>
<th>WAN</th>
<th>WAN Setup - Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>xDSL Properties</td>
<td>Make sure that the settings below match the settings provided by your ISP.</td>
</tr>
<tr>
<td>WAN IP: ATM</td>
<td>Connection Type: Stop</td>
</tr>
<tr>
<td>WAN IP: PTM</td>
<td></td>
</tr>
<tr>
<td>WAN IP: Ethernet</td>
<td></td>
</tr>
<tr>
<td>WAN IP Services</td>
<td></td>
</tr>
</tbody>
</table>

Click "Apply/Save" to have this interface be effective. Click "Back" to make any modifications.
SECTION 2.6 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)

Enable IPv6: Only Dual Stack supported

Once complete, select “Next”
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”

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
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”
SECTION 2.7 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 IF: Services](image)

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”
2.D Specify WAN IP Settings

PPP Authentication Client
Username
Password
MTU: 1492
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”
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”
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

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 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”.

VisionNet M405 R3
Page 27 of 52
User Manual Rev 0.1.2
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:

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:

- **Bridged Service Group**
  - ADSL2+ ATM 0.35

- **MGMT Service Group**
  - ADSL2+ ATM 0.32

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

- **Bridged Internet Service Group**
  - 192.168.2.1
  - Ethernet 0

- **MGMT Service Group**
  - 192.168.1.1
  - USB; Gateway Management 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

The most common use, for the M405 Service Grouping, is to isolate a bridged connection; which providing a second connection for Management.
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:

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.

NOTE: IF YOU ARE CONNECTED TO THE ETHERNET PORT, AND YOU ISOLATE THE ETHERNET PORT FROM THE DEFAULT GROUP, YOU MUST REFRESH YOUR IP; AND CONNECT VIA THE NEW GATEWAY

DHCP Vendor IDs

This is the BootP, Option 60, ID

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.

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 multicast 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 page](image)

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

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

---

VisionNet M405 R3  Page 31 of 52  User Manual Rev 0.1.2
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 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“.
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  
1.A  Direct your browser to the IF Default Gateway page

Step 2  
2.A  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 “.
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"

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

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:

![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.

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

![VisionNet M405 R3]

Page 35 of 52  User Manual Rev 0.1.2
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:

![IF Default DNS](image)

Step 2 Statically Assign DNS Servers

2.A Select IFs “Use the following statically assigned IPv4 DNS Servers”.

IPv4

Enter Primary and Secondary

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: 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.

2.B  NAT

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:

Multi-NAT

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:

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:

Step 2  Create Port Triggering Rules

2.A Select “Add”

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

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:

DMZ Host

Step 2  Specify DMZ Host

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

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

Step 2  Enable / Disable requested ALG

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

Step 3  When finished, select “Apply / Save”. 
SECTION 9: PUBLIC IPv4 LAN ASSIGNMENT

SECTION 9.1 Routed IPv4 Subnet Allocation (With Security Considerations)

Abstract

This section will describe a standard /29 routed subnet allocation to LAN hosts. The procedures are virtually identical whether PPP or IPoE WAN Interfaces are used.

It is suggested that this entire section be reviewed prior to implementation.

Step 1 During WAN Configuration

1.A General Notes:

/29 May be allocated using PPP or IPoE

/29 May be allocated using Static or Dynamically assigned IPs

NAT - DISABLED

FIREWALL - ENABLED
This will enforce Management for the Gateway, and prevent security attacks. We will need to apply rules to allow inbound host traffic.
Step 2  LAN Configuration

General Notes:

Routed Subnet IPs may be dynamic or statically.

The first usable host should be assigned to the Gateway’s LAN IP.

Hosts must use the Gateway’s LAN IP as the default gateway.

If Dynamic IPs are used, it is preferred that the host be entered into the Static IP Lease table.

Step 3  CPE MANAGEMENT INTERFACES

Admin Services:

WAN Services may be accessed via the public IP assigned to the WAN Interface.

LAN Services are accessible to LAN Hosts. If the WAN Service Firewall is not enabled, then all DNS and Management services will be exposed.

Service ACL:

IP Acess Control Lists, if applied, must be updated prior to making any changes to the LAN Subnet.
LAN HOSTS FIREWALL CONSIDERATIONS

Step 4

Allow Inbound Traffic:
Null sections will be left un-restricted.

Two Firewall entries must be placed for each host. One for TCP/UDP; the other for ICMP

Best Practices Include:
Each IP to be applied individually, to ensure that the IT Administrator may control access.

IE: Ingress Rules
IPv4 XXX.XXX.XXX.XXX/32 TCP/UDP
IPv4 XXX.XXX.XXX.XXX/32 ICMP
SECTION 9.2 Multi-NAT

Abstract

Multi-NAT is designed to bypass NAT applications, so that a Public IP may be forwarded to LAN IPs.

This is designed for applications where a Public IP should correlate to a private designed host.

Step 1  Direct your browser to the Multi-NAT page

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

   Multi-NAT

Step 2  Multi-NAT Table Application

2.A Rule Type:

   1:1NAT - This creates a 1 to 1 corollary between a public IP, and private IP. Any IP forwarded to the CPE will be forwarded to the specified private host.

   1:Many NAT - Traffic directed to one IP will be forwarded to a sequential list of IPs

   Many : 1 NAT - Traffic directed to multiple IPs will be directed to a single host

   Many : Many: Traffic directed to multiple Public IPs will be directed to Multiple LAN IPs.

2.B When finished, select "Apply / Save".
SECTION 10 Product Specifications

SECTION 10.1 Product Specifications

**WAN Interface Features**
- T1.413
- G.Lite
- G.DMT
- G.Bond (ADSL2+/VDSL2)
- ADSL2 / ADSL2+
- SRA
- Bitswap
- AAL5, UNI 3.1/4, F4/F5
- Annex A
- Annex L
- Annex M
- PhyR / G.INP
- Nitro
- ATM
- Adjustable MTU
- UBR/CBR/VBR-rt/nrt

**LAN Service Features**
- Inter LAN Routing
- Multiple DHCP Servers
- MAC Reservation
- UPnP
- IPv4, IPv6, Dual Stack
- Isolated LAN Networks
- Service Grouping
- Secondary Subnetting
- IGMP Snoop / Block
- Enhanced IGMP
- IGMP Customization
- 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

**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

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

**Hardware Specifications**

**WAN:** xDSL

**LAN:** 1 Port 10 / 100 FE

**USB:** 1.1 Type Mini B – Management

**Power:** 5VDC / 110-220VAC, 50~60Hz

**Temp:** 0 - 65C, Humidity: 5 ~ 95% (non-condensing)
SECTION 10.2 Product Depictions

Front Depiction

![Front Depiction Image]

Back Depiction

![Back Depiction Image]

Label Depiction

![Label Depiction Image]
## SECTION 10.3 LED Functionality

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong></td>
<td>Status Power / Router</td>
<td>Solid Green – Power On&lt;br&gt;Off – Power Off&lt;br&gt;Flashing Green 2 hz – Flashing Power on self test</td>
</tr>
<tr>
<td><strong>Ethernet</strong></td>
<td>Status Ethernet Port</td>
<td>Off - Power Off – or – No Powered device detected&lt;br&gt;Solid Green – Powered device connected ; including wake on LAN&lt;br&gt;Flashing Green – LAN activity present for that port</td>
</tr>
<tr>
<td><strong>DSL</strong></td>
<td>Status DSL Link Line 1</td>
<td>Green – DSL Good Sync&lt;br&gt;Off - Powered off&lt;br&gt;Flashing Green - DSL Attempting sync&lt;br&gt;Signal Detection – Flashing 2hz with 50% duty cycle&lt;br&gt;Carrier Detected, Modem training – Flashing at 4hz with 50% duty cycle</td>
</tr>
<tr>
<td><strong>Internet</strong></td>
<td>Status Internet Connection</td>
<td>Solid Green – IP connected – no traffic passing&lt;br&gt;Device has a WAN IP via either static/ DHCP/ or IPCP&lt;br&gt;If PPP is used, device has authenticated and has a WAN IP Address&lt;br&gt;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.&lt;br&gt;Off – No Internet Detected&lt;br&gt;LED Should remain off if modem is in bridged mode or if DSL Connection is not present&lt;br&gt;Flashing Green – Device has WAN IP Address and IP Traffic is passing through device</td>
</tr>
<tr>
<td><strong>USB</strong></td>
<td>Status Internet Connection</td>
<td>Off – No connected device&lt;br&gt;Solid Green – Device Connected</td>
</tr>
</tbody>
</table>
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: M405R3  
FCC ID: QMPM405R3  
US: DQ1DL01BM405R3

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 20cm between the radiator and your body.

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

Note: 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 communication. However, there is no guarantee this 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:AAAAEQ## 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: DQ1DL01BM405R3] 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 isn't 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: DQ1DL01BM405R3], 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
   Tel: +1 925 730 3940

   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 [M405R3] 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: DQ1DL01BM405R3]
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 numbers [US: DQ1DL01BM405R3] indicates the REN would be 0.1.