Quality of Service (QoS)
Differentiated Services Rules, Internet Protocol Range Rules, Medium Access Control Range Rules and Virtual Local Area Network Rules for Net to Net's Network Management System

![Circuit Configuration - Microsoft Internet Explorer](image)

1. When allow tag on ingress pkt, the port acts as 802.1Q VLAN trunk, otherwise the port acts as 802.1Q VLAN access.
2. Add a single VLAN tag to the ingress pkt when 'Allow' Tag/Tag on Ingress Pkt is not to untag.
3. The 'Fixed/Max' attribute will be applied to the VLAN priority when 'Allow' Tag/Tag on Ingress Pkt is set to tag.
Contents

1.0 BACKGROUND

1.1 DEFINITIONS
   1.1.1 Ingress Packet
   1.1.2 Egress Packet

2.0 OVERVIEW

2.1 Packets with a VLAN Tag
   2.1.1 OSI Layer 3: Diffserv and IP Range Rules
   2.1.2 OSI Layer 2: MAC Range and VLAN Rules

2.2 Packets without a VLAN Tag
   2.2.1 OSI Layer 3: Diffserv and IP Range Rules
   2.2.2 OSI Layer 2: MAC Range and VLAN Rules

3.0 NMS v2.1

4.0 SINGLE CIRCUIT QoS RULES

4.1 DSCP & IP Rules
   4.1.1 Select Port for Configuration
   4.1.2 Circuit Configuration Diffserv Rules
      4.1.2.1 Activate Rule
      4.1.2.2 Differentiated Services (DS) Value and Mask
      4.1.2.3 Allow Tag or Untag on Ingress Packets
      4.1.2.4 VLAN
      4.1.2.5 Add VLAN Tag to Ingress Packets
      4.1.2.6 Priority
      4.1.2.7 Fixed or Maximum Priority
      4.1.2.8 Ingress and Egress Limits
      4.1.2.9 Matching Packets with a Diffserv Rule
   4.1.3 Circuit Configuration IP Range Rules
      4.1.3.1 Activate Rule
      4.1.3.2 IP Range
      4.1.3.3 Allow Tag or Untag on Ingress Packets
      4.1.3.4 VLAN
      4.1.3.5 Add VLAN Tag to Ingress Packets
      4.1.3.6 Priority
      4.1.3.7 Fixed or Maximum Priority
      4.1.3.8 Ingress and Egress Limits
      4.1.3.9 Matching Packets with an IP Range Rule
   4.1.4 Submit Circuit Diffserv & IP Range Rules
   4.1.5 Reset Circuit Diffserv & IP Range Rules

4.2 MAC Rules
   4.2.1 Select Port for Configuration
   4.2.2 Circuit Configuration MAC Rules
      4.2.2.1 Activate Rule
      4.2.2.2 MAC Range
      4.2.2.3 Allow Tag or Untag on Ingress Packets
      4.2.2.4 VLAN
      4.2.2.5 Add VLAN Tag to Ingress Packets
      4.2.2.6 Priority
      4.2.2.7 Fixed or Maximum Priority
      4.2.2.8 Ingress and Egress Limits
      4.2.2.9 Matching Packets with a MAC Rule
   4.2.3 Submit Circuit MAC Rules
   4.2.4 Reset Circuit MAC Rules

4.3 VLAN Rules
   4.3.1 Select Port for Configuration
   4.3.2 Circuit Configuration VLAN Rules
      4.3.2.1 Activate Rule
      4.3.2.2 Allow Tag or Untag on Ingress Packets
      4.3.2.3 VLAN
4.3.2.4 Add VLAN Tag to Ingress Packets
4.3.2.5 Priority
4.3.2.6 Fixed or Maximum Priority
4.3.2.7 Ingress and Egress Limits
4.3.2.8 Matching Packets with a VLAN Rule

4.3.3 Backbone and Flood
4.3.3.1 Backbone Ethertype
4.3.3.2 Backbone VLAN ID
4.3.3.3 Flood

4.3.4 Submit Circuit VLAN Rules
4.3.5 Reset Circuit VLAN Rules

5.0 GLOBAL QoS RULES

5.1 Global DSCP & IP Rules
5.1.1 Select Slot(s) and Port(s) for Configuration
  5.1.1.1 Slot
  5.1.1.2 Add Slot(s)
  5.1.1.3 Add Port(s)
5.1.2 Global Configuration Diffserv Rules
  5.1.2.1 Add, Delete or Do Not Set
  5.1.2.2 Activate Rule
  5.1.2.3 Differentiated Services (DS) Value and Mask
  5.1.2.4 Allow Tag or Untag on Ingress Packets
  5.1.2.5 VLAN
  5.1.2.6 Add VLAN Tag to Ingress Packets
  5.1.2.7 Priority
  5.1.2.8 Fixed or Maximum Priority
  5.1.2.9 Ingress and Egress Limits
  5.1.2.10 Matching Packets with a Diffserv Rule
5.1.3 Global Configuration IP Range Rules
  5.1.3.1 Add, Delete or Do Not Set
  5.1.3.2 Activate Rule
  5.1.3.3 IP Range
  5.1.3.4 Allow Tag or Untag on Ingress Packets
  5.1.3.5 VLAN
  5.1.3.6 Add VLAN Tag to Ingress Packets
  5.1.3.7 Priority
  5.1.3.8 Fixed or Maximum Priority
  5.1.3.9 Ingress and Egress Limits
  5.1.3.10 Matching Packets with an IP Range Rule
5.1.4 Submit Global Diffserv & IP Range Rules
5.1.5 Reset Global Diffserv & IP Range Rules

5.2 Global MAC Rules
5.2.1 Select Slot(s) and Port(s) for Configuration
  5.2.1.1 Slot
  5.2.1.2 Add Slot(s)
  5.2.1.3 Add Port(s)
5.2.2 Global Configuration MAC Rules
  5.2.2.1 Add, Delete, Do Not Set
  5.2.2.2 Activate Rule
  5.2.2.3 MAC Range
  5.2.2.4 Allow Tag or Untag on Ingress Packets
  5.2.2.5 VLAN
  5.2.2.6 Add VLAN Tag to Ingress Packets
  5.2.2.7 Priority
  5.2.2.8 Fixed or Maximum Priority
  5.2.2.9 Ingress and Egress Limits
  5.2.2.10 Matching Packets with a MAC Rule
5.2.3 Submit Global MAC Rules
5.2.4 Reset Global MAC Rules

5.3 Global VLAN Rules
5.3.1 Select Slot(s) and Port(s) for Configuration
  5.3.1.1 Slot
  5.3.1.2 Add Slot(s)
  5.3.1.3 Add Port(s)
5.3.2 Global Configuration VLAN Rules
  5.3.2.1 Add, Delete or Do Not Set
  5.3.2.2 Activate Rule
  5.3.2.3 Allow Tag or Untag on Ingress Packets
  5.3.2.4 VLAN
  5.3.2.5 Add VLAN Tag to Ingress Packets
  5.3.2.6 Priority
  5.3.2.7 Fixed or Maximum Priority
1.0 BACKGROUND

Prior to the availability of these Quality of Service (QoS) features, Net to Net’s DSLAMs processed packets by a set of largely non-configurable default rules. With the release of the current QoS features however, configuration is allowed at both the Layer 2 and Layer 3 levels of the Open Systems Interconnection (OSI) model. OSI is an internationally accepted framework of standards for communication between different network systems and vendors that organizes the communication process into seven [7] different layers. Layer 3, the Network Layer, dictates how data should be transferred within and between systems. Layer 2, the Data Link Layer, dictates the procedures and protocols to be used in operating the network lines.

1.1 DEFINITIONS

1.1.1 Ingress Packet
An incoming packet; a packet coming in from a subscriber or uplink connection.

1.1.2 Egress Packet
An outgoing packet; a packet going out over a subscriber or uplink connection.

2.0 OVERVIEW

Net to Net’s QoS features enable network operators to specify four [4] types of rules to guide a DSLAM’s handling of packets. There are two [2] OSI Layer 3 rules, Differentiated Services (Diffserv) Rules and Internet Protocol (IP) Range Rules, as well as two [2] OSI Layer 2 rules, Medium Access Control (MAC) Range Rules and Virtual Local Area Network (VLAN) Rules. Once the QoS rules have been configured, the DSLAM will attempt to match each packet to one of the QoS Rules in the following order:

1. Diffserv Rules (up to 4 rules may be configured)
2. IP Range Rules (up to 4 rules may be configured)
3. MAC Rules (up to 4 rules may be configured)
4. VLAN Rules (up to 10 rules may be configured)

In other words, the DSLAM will first attempt to match a packet to a configured Diffserv Rule. If the packet does not match any of the Diffserv Rules, the DSLAM will then attempt to match the packet to one of the port’s configured IP Range Rules.
If a packet does not match any of a port's configured DiffServ or IP Range Rules, the DSLAM will then attempt to match the packet to one of the port's configured MAC Rules. If the packet does not match any of the MAC Rules, the DSLAM will then attempt to match the packet to one of the port's configured VLAN Rules.

Once a match is made between a packet and a QoS Rule, that packet is categorized according to the rule with which it was matched (DiffServ, IP, MAC or VLAN) and no further matching attempts are made. If a packet does not match ANY of the activated QoS rules for a port, it will be dropped. If no QoS rules have been activated for a port, ALL traffic will be allowed to pass through that port.
2.1 Packets with a VLAN Tag

2.1.1 OSI Layer 3: Diffserv and IP Range Rules
A packet, with a VLAN tag, that has been matched to one of a port's Diffserv or IP Range Rules will be forwarded if the packet's VLAN tag falls within the configured VLAN range of that Diffserv or IP Range Rule; if the packet's VLAN tag does not fall within the configured VLAN range of that Diffserv or IP Range Rule then the packet will be dropped.

NOTE: If a packet's VLAN tag does not fall within the VLAN range of the Diffserv or IP Range Rule to which it has been matched, the packet will be dropped, even if the tag does fall within the VLAN range of a rule further down the chain.

2.1.2 OSI Layer 2: MAC Range and VLAN Rules
A packet, with a VLAN tag, that has been matched to one of a port's MAC Rules will be forwarded if the packet's VLAN tag falls within the configured VLAN range of that MAC Rule; if the packet's VLAN tag does not fall within the configured VLAN range of that MAC Rule then the packet will be dropped.

NOTE: If a packet's VLAN tag does not fall within the VLAN range of the MAC Rule to which it has been matched, the packet will be dropped, even if the tag does fall within the VLAN range of a rule further down the chain.
A packet, with a VLAN tag, that has not already been matched with one of a port's Diffserv, IP Range or MAC Rules will be matched to the FIRST VLAN Rule for which the packet's VLAN tag falls within the configured VLAN range of that rule; if the packet's VLAN tag does not fall within the configured VLAN range of ANY of the port's VLAN Rules then the packet will be dropped.

2.2 Packets without a VLAN Tag

2.2.1 OSI Layer 3: Diffserv and IP Range Rules
A packet, without a VLAN tag, that has been matched to one of a port's Diffserv or IP Range Rules will be forwarded if that Diffserv or IP Range Rule is configured NOT to allow packets with a VLAN tag (untag); if the Diffserv or IP Range Rule to which the packet has been matched IS configured to allow packets with a VLAN tag (tag) then the packet will be dropped.
2.2.2 OSI Layer 2: MAC Range and VLAN Rules

A packet, without a VLAN tag, that has been matched to one of a port's MAC Rules will be forwarded if the MAC Rule is configured NOT to allow packets with a VLAN tag (untag); if the MAC Rule to which the packet has been matched IS configured to allow packets with a VLAN tag (tag) then the packet will be dropped.

A packet, without a VLAN tag, that has not already been matched to a Diffserv, IP Range or MAC Rule will automatically be matched to a port’s untag VLAN Rule; if none of the port’s VLAN Rules are configured to allow packets without a VLAN tag (untag) then the packet will be dropped.

**NOTE** No more than one VLAN Rule per port should be configured to allow packets without a VLAN tag (untag); any untagged packets that have not already been matched to a Diffserv, IP Range or MAC Rule will automatically be matched with the FIRST VLAN Rule that allows untagged packets. Therefore, any subsequent VLAN Rules allowing untagged packets will not be utilized.
3.0 NMS v2.1

Open a Network Management System (NMS) window and log on. You must log on as a Superuser in order to make QoS and VLAN configurations.

Net to Net’s DEFAULT Superuser logon is as follows:

Username: "superuser"
Password: "Password"

Both username and password are case sensitive.

4.0 SINGLE CIRCUIT QoS RULES

From the NMS main window, click on any one of the port LEDs depicted on the DSLAM image to get to the Circuit Configuration window.
4.1 DSCP & IP Rules

Click on the DSCP & IP Rules tab at the top of the Circuit Configuration window.

4.1.1 Select Port for Configuration

Using the pull-down menus, select the slot number and port number of the port for which you wish to configure a Diffserv or IP Range Rule. The Slot pull-down menu will only list the DSLAM slots that are occupied by an interface module; empty slots and slots occupied by blank plates will not be listed. The slot selected will be detailed in the Device Type and Revision fields. In the following illustration, Port 11 in Slot 2 has been chosen for configuration; Slot 2 contains a SIM2000-24 with firmware revision 2.00.00.
4.1.2 Circuit Configuration Diffserv Rules

A Differentiated Services Code Point (DSCP) provides OSI Layer 3 identification information within a packet's IP header for the purpose of determining packet type. Up to four [4] separate Differentiated Services (Diffserv) Rules may be configured per port.

**NOTE** Ethertype 0x800 IP packets are the only type of packets that can be matched with Diffserv Rules.
4.1.2.1 Activate Rule

A Diffserv Rule will not be applied to the selected port unless it is activated. Use the pull-down menu to select either yes or no. Default is no.

**NOTE** You may wish to submit (Section 4.1.4) an added Diffserv Rule and then review your parameter configurations prior to activation.

4.1.2.2 Differentiated Services (DS) Value and Mask

4.1.2.2.1 DS Value

The DS Value of a packet is a hexadecimal value calculated from the upper six [6] bits of an eight [8] bit field in the packet’s IP header (the remaining two [2] bits are unused) known as the Differentiated Services Code Point (DSCP). It is one of several methods used to determine packet type. Configuring a DS Value requires knowledge of your (desired) network traffic and, as such, a default value is not applicable (indicated as 00).

**NOTE** Though it is only the upper six bits of the eight bit field in a packet’s IP header that comprise the DSCP, DS Value calculations require that all eight bits be configured nonetheless.
4.1.2.2 DS Mask
The DS Mask is a hexadecimal value that indicates which of the DSCP's upper six [6] bits will be utilized in considering a packet's DSCP type. Default is FC, indicating that ALL of the DSCP's upper six bits will be used in calculating the packet's DS Value.

How It Works:
A "logical bit-wise AND" is performed between a packet's DSCP and the DS Mask value of the Diffserv Rule. The result must equal the DS Value configured for that Diffserv Rule in order for the packet to match the DS Value portion of that rule.

4.1.2.3 Allow Tag or Untag on Ingress Packets
Use the pull-down menu to select either tag or untag. Tag indicates that ingress packets already matched to the Diffserv Rule must have a VLAN tag to be further considered; packets without a VLAN tag will be dropped. Untag indicates that ingress packets already matched to the Diffserv Rule cannot have a VLAN tag to be further considered; packets with a VLAN tag will be dropped. Default is untag.

4.1.2.4 VLAN
For each individual Diffserv Rule, if you selected tag in Section 4.1.2.3, the VLAN field should specify either an acceptable Single VLAN, or an acceptable VLAN Range, for VLAN tags on ingress packets. If you selected untag, the VLAN field should specify a Single VLAN only if you intend to have a VLAN tag added to packets (Section 4.1.2.5); if you do not intend to have a VLAN tag added to packets, the VLAN field should be left at the 0-0 default.

4.1.2.4.1 Single VLAN
If tag was selected in Section 4.1.2.3, only packets with the specified VLAN tag will match the VLAN portion of the Diffserv Rule. If untag was selected, a Single VLAN should only be specified if the Diffserv Rule is also configured to add a VLAN tag to packets (Section 4.1.2.5).

For a packet that has already been matched to a Diffserv Rule:

<table>
<thead>
<tr>
<th>Allow Tag/Untag on Ingress Pkt.</th>
<th>and the Ingress Packet has</th>
<th>the result will be</th>
<th>and the Egress Packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>no VLAN tag match</td>
<td>have the configured VLAN tag added</td>
<td></td>
</tr>
<tr>
<td>any VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

Start Tag = End Tag
4.1.2.4.2 VLAN Range
A VLAN range should only be specified if tag was selected in Section 4.1.2.3. Only packets tagged within the specified VLAN range will match the VLAN portion of the Diffserv Rule. If a VLAN Range is specified, the Diffserv Rule MUST be configured to allow packets to continue on with the same VLAN tag they came in with (Section 4.1.2.5).

For a packet that has already been matched to a Diffserv Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td>no VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>the specified VLAN tag</td>
<td>match</td>
<td>keep the same VLAN tag</td>
<td></td>
</tr>
<tr>
<td>any VLAN tag other than the specified VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

4.1.2.5 Add VLAN Tag to Ingress Packets
Use the pull-down menu to select either yes or no. Default is no.

For a packet that has already been matched to a Diffserv Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the Diffserv Rule must be configured with a single VLAN (Section 4.1.2.4.1) and a VLAN tag with the specified value will be added to the packet</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>the packet will continue on without a VLAN tag</td>
</tr>
<tr>
<td>tag</td>
<td>yes*</td>
<td>the packet will continue on with the same VLAN tag it had at ingress</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 4.1.2.3).
4.1.2.6 Priority
Use the pull-down menu to select a priority value from 0 - 7, where 0 is no priority, 1 is the lowest priority and 7 is the highest priority. Default is 0.

For a packet that has come in through a subscriber connection and has already been matched to a Diffserv Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the Diffserv Rule Priority will be added to the packet as part of the VLAN tag and will be applied to the packet both within the DSLAM and at egress</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>the packet will follow the Diffserv Rule Priority within the DSLAM only; it will not be added to the packet at egress</td>
</tr>
<tr>
<td>tag</td>
<td>yes*</td>
<td>Priority will be applied according to the Diffserv Rule Fixed/Max configuration (Section 4.1.2.7)</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 4.1.2.3).

**NOTE** Diffserv Rule Priority configurations do not apply to packets that have come in through an uplink connection; packets coming from an uplink connection will retain their original priority.

4.1.2.7 Fixed or Maximum Priority
The Fixed/Max field dictates the action to be taken with the configured Priority (Section 4.1.2.6) of a tagged packet that has come in through a subscriber connection and has already been matched to a Diffserv Rule. Use the pull-down menu to select either fixed or max. Default is fixed.

4.1.2.7.1 Fixed (default)
The packet's original priority will automatically be replaced with the Diffserv Rule Priority (Section 4.1.2.6).

4.1.2.7.2 Max
The packet's original priority will only be replaced with the configured Diffserv Rule Priority (Section 4.1.2.6) if the packet's original priority is
greater than the Diffserv Rule Priority. E.g. If the Diffserv Rule Priority has
been configured at 4, a packet’s original priority will be replaced only if it is
greater than 4 (as in 5, 6 or 7).

**NOTE** The Diffserv Fixed/Max parameter does not apply to packets that have come in through an uplink connection;
neither will the Fixed/Max configuration come into play if a QoS Backbone VLAN ID (Section 4.3.3.2) has been
configured.

4.1.2.8 **Ingress and Egress Limits**
Ingress Limit and Egress Limit allow traffic-specific, rule-specific, bandwidth limits
to be set for each port. Unit of measure is kbps. Default is 0 (no limit).

![DiffServ Rule Settings Table](image)

4.1.2.9 **Matching Packets with a Diffserv Rule**
The first step in matching a packet with a Diffserv Rule is matching the DS Value.
Once it has been determined that a packet matches the DS Value of a Diffserv Rule,
that packet must then match all other criteria for that rule as well, or it will be
dropped. If a packet does not match the DS Value of a rule, it will be passed on for
an attempted match with the next rule in line.

**NOTE** If a packet matches a Diffserv Rule’s DS Value but fails to match one or more of the other criteria for that rule,
it will be dropped; it will not continue on to the next rule.

4.1.2.9.1 **Packets with a VLAN Tag**
When Allow Tag/Untag on Ingress Pkt. is set to *tag* (Section 4.1.2.3), a tagged
packet with a DS Value and VLAN that match the configurations of a Diffserv
Rule will be deemed a match with that rule and no further attempts will be
made to match that packet with any other QoS Rules. Additionally, once a
packet has been matched with a Diffserv Rule, it will conform to the priority
and bandwidth limits as configured for that rule.

![Packets with a VLAN Tag Diagram](image)

*If a QoS Rule Backbone VLAN has been configured, then the Backbone VLAN will be taken into consideration
along with the standard VLAN in determining whether a packet matches a Diffserv Rule. Refer to Section 4.3.3.2
for further information regarding Backbone VLAN.

4.1.2.9.2 **Packets without a VLAN Tag**
When Allow Tag/Untag on Ingress Pkt. is set to *untag* (Section 4.1.2.3), an
untagged packet with a DS Value that matches the configurations of a
Diffserv Rule will be deemed a match with that rule and no further attempts
will be made to match that packet with any other QoS Rules. Additionally,
once a packet has been matched with a Diffserv Rule, it will conform to the VLAN and priority configurations, as well as bandwidth limits, as configured for that rule.

4.1.3 Circuit Configuration IP Range Rules

Internet Protocol (IP) address ranges are a method of providing OSI Layer 3 identification information for prioritization purposes. Packet priority is assigned based on the source and/or destination IP address of the packet. Up to four [4] separate IP address Rules may be configured per port.

**NOTE** Ethertype 0x800 and 0x806 IP packets are the only type of packets that can be matched with IP Range Rules.

4.1.3.1 Activate Rule

An IP Range Rule will not be applied to the selected port unless it is activated. Use the pull-down menu to select either yes or no. Default is no.
4.1.3.2 IP Range
Packets containing a source and/or destination IP address that falls within the configured range will match the IP portion of the IP Range Rule. Default is 0.0.0.0 - 0.0.0.0. No packets will match at the default IP Range setting; you must configure the IP Range as is appropriate for your individual network.

4.1.3.2.1 Single IP Address
Only packets with the specified IP address, as either their source or destination, will match the IP address portion of the IP Range Rule.

```
<table>
<thead>
<tr>
<th>IP Range</th>
<th>Start IP = End IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>193.166.254.98</td>
<td>193.166.254.98</td>
</tr>
</tbody>
</table>
```

4.1.3.2.2 IP Range
Only packets with a source and/or destination IP address within the specified range will match the IP address portion of the IP Range Rule.

```
<table>
<thead>
<tr>
<th>IP Range</th>
<th>Start IP &lt; End IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>193.166.254.98</td>
<td>193.166.254.254</td>
</tr>
</tbody>
</table>
```

4.1.3.2.3 Full IP Range
All packets will match the IP portion of the IP Range Rule.

```
<table>
<thead>
<tr>
<th>IP Range</th>
<th>Start IP = 0.0.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>
```

4.1.3.3 Allow Tag or Untag on Ingress Packets
Use the pull-down menu to select either *tag* or *untag*. *Tag* indicates that ingress packets already matched to the IP Range Rule must have a VLAN tag to be further considered; packets without a VLAN tag will be dropped. *Untag* indicates that ingress packets already matched to the IP Range Rule cannot have a VLAN tag to
be further considered; packets with a VLAN tag will be dropped. Default is *untag*.

### 4.1.3.4 VLAN

For each individual IP Range Rule, if you selected *tag* in Section 4.1.3.3, the VLAN field should specify either an acceptable Single VLAN, or an acceptable VLAN Range, for VLAN tags on ingress packets. If you selected *untag*, the VLAN field should specify a Single VLAN only if you intend to have a VLAN tag added to packets (Section 4.1.3.5); if you do not intend to have a VLAN tag added to packets, the VLAN field should be left at the 0 - 0 default.

#### 4.1.3.4.1 Single VLAN

If *tag* was selected in Section 4.1.3.3, only packets with the specified VLAN tag will match the VLAN portion of the IP Range Rule. If *untag* was selected, a Single VLAN should only be specified if the IP Range Rule is also configured to add a VLAN tag to packets (Section 4.1.3.5).

For a packet that has already been matched to an IP Range Rule:

<table>
<thead>
<tr>
<th>VLAN (1-4085)</th>
<th>Start Tag = End Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>999</td>
<td>993</td>
</tr>
</tbody>
</table>

**if Allow Tag/UnTag on Ingress Pkt. is configured as**

<table>
<thead>
<tr>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td></td>
<td></td>
</tr>
<tr>
<td>no VLAN tag</td>
<td>match</td>
<td>have the configured VLAN tag added</td>
</tr>
<tr>
<td>any VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
</tr>
<tr>
<td>tag</td>
<td></td>
<td></td>
</tr>
<tr>
<td>no VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
</tr>
<tr>
<td>the specified VLAN tag</td>
<td>match</td>
<td>keep the same VLAN tag</td>
</tr>
<tr>
<td>any VLAN tag other than the specified VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
</tr>
</tbody>
</table>

#### 4.1.3.4.2 VLAN Range

A VLAN range should only be specified if *tag* was selected in Section 4.1.3.3. Only packets tagged within the specified VLAN range will match the VLAN portion of the IP Range Rule. If a VLAN range is specified, the IP Range Rule MUST be configured to allow packets to continue on with the same VLAN tag they came in with (Section 4.1.3.5).
4.1.3.5  Add VLAN Tag to Ingress Packets
Use the pull-down menu to select either yes or no. Default is no.

For a packet that has already been matched to an IP Range Rule:

<table>
<thead>
<tr>
<th>VLAN Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td>no VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>any VLAN tag within the specified range</td>
<td>match</td>
<td>keep the same VLAN tag</td>
<td></td>
</tr>
<tr>
<td>any VLAN tag not in the specified range</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

Start Tag < End Tag

For a packet that has already been matched to an IP Range Rule:

if Allow Tag/Untag on Ingress Pkt. is configured as and Add VLAN to Ingress Pkt. is configured as then

<table>
<thead>
<tr>
<th>VLAN Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the IP Range Rule must be configured with a single VLAN (Section 4.1.3.4.1) and a VLAN tag with the specified value will be added to the packet</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>the packet will continue on without a VLAN tag</td>
</tr>
<tr>
<td>tag</td>
<td>yes*</td>
<td>the packet will continue on with the same VLAN tag it had at ingress</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 4.1.3.3).

4.1.3.6  Priority
Use the pull-down menu to select a priority value from 0 - 7, where 0 is no priority, 1 is the lowest priority and 7 is the highest priority. Default is 0.

For a packet that has already been matched to an IP Range Rule:

<table>
<thead>
<tr>
<th>VLAN Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tag</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.1.3.7 Fixed or Maximum Priority
The Fixed/Max field dictates the action to be taken with the configured Priority (Section 4.1.3.6) of a tagged packet that has come in through a subscriber connection and has already been matched to an IP Range Rule. Use the pull-down menu to select either fixed or max. Default is fixed.

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the IP Range Rule Priority will be added to the packet as part of the VLAN tag and will be applied to the packet both within the DSLAM and at egress</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>the packet will follow the IP Range Rule Priority within the DSLAM only; it will not be added to the packet at egress</td>
</tr>
<tr>
<td>tag</td>
<td>yes*</td>
<td>Priority will be applied according to the IP Range Rule Fixed/Max configuration (Section 4.1.3.7)</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 4.1.3.3).

**NOTE** IP Range Rule Priority configurations do not apply to packets that have come in through an uplink connection; packets coming from an uplink connection will retain their original priority.

4.1.3.7.1 Fixed (default)
The packet's original priority will automatically be replaced with the IP Range Rule Priority (Section 4.1.3.6).

4.1.3.7.2 Max
The packet's original priority will only be replaced with the configured IP Range Rule Priority (Section 4.1.3.6) if the packet's original priority is greater than the IP Range Rule Priority. E.g. If the IP Range Rule Priority has been configured at 4, a packet's original priority will be replaced only if it is greater than 4 (as in 5, 6 or 7).

**NOTE** The IP Range Rule Fixed/Max parameter does not apply to packets that have come in through an uplink connection; neither will the Fixed/Max configuration come into play if a QoS Backbone VLAN ID (Section 4.3.3.2) has been configured.

4.1.3.8 Ingress and Egress Limits
Ingress Limit and Egress Limit allow traffic-specific, rule-specific, bandwidth limits to be set for each port. Unit of measure is kbps. Default is 0 (no limit).
4.1.3.9 Matching Packets with an IP Range Rule

The first step in matching a packet with an IP Range Rule is matching the destination and/or source IP address. Once it has been determined that a packet's destination and/or source IP address matches the configured Single IP or IP Range of an IP Range Rule, it must then match all other criteria for that rule as well, or the packet will be dropped. If a packet's destination and/or source IP address does not match the Single IP or IP Range of an IP Range Rule, the packet will be passed on for an attempted match with the next rule in line.

**NOTE** If a packet's destination and/or source IP address matches the Single IP or IP Range of an IP Range Rule but fails to match one or more of the other criteria for that rule, it will be dropped; it will not continue on to the next rule.

4.1.3.9.1 Packets with a VLAN Tag

When Allow Tag/Untag on Ingress Pkt. is set to *tag* (Section 4.1.3.3), a tagged packet with an IP address and VLAN that match the configurations of an IP Range Rule will be deemed a match with that rule and no further attempts will be made to match that packet with any other QoS Rules. Additionally, once a packet has been matched with an IP Range Rule, it will conform to the priority and bandwidth limits as configured for that rule.

4.1.3.9.2 Packets without a VLAN Tag

When Allow Tag/Untag on Ingress Pkt. is set to *untag* (Section 4.1.3.3), an untagged packet with an IP address that matches the configurations of an IP Range Rule will be deemed a match with that rule and no further attempts will be made to match that packet with any other QoS Rules. Additionally, once a packet has been matched with an IP Range Rule, it will conform to the VLAN and priority configurations, as well as bandwidth limits, as configured for that rule.

*If a QoS Rule Backbone VLAN has been configured, then the Backbone VLAN will be taken into consideration along with the standard VLAN in determining whether a packet matches an IP Range Rule. Refer to Section 4.3.3.2 for further information regarding Backbone VLAN.*
4.1.4 Submit Circuit DiffServ & IP Range Rules
Once all parameters in the Circuit Configuration DSCP & IP Rules window have been configured as desired, click the submit button at the bottom of the window. Any configurations that are not submitted will be discarded. If any accidental or undesirable changes have been made, exit the screen without clicking submit and the changes will be discarded. If any accidental or undesirable changes have already been submitted, simply make the desired adjustments and then resubmit the rule.

4.1.5 Reset Circuit DiffServ & IP Range Rules
Resetting a port's Diffserv and IP Range Rules will return ALL of that port's Diffserv AND IP Range Rules to their original default settings; Diffserv and IP Range Rules cannot be reset individually. Click the box to the left of the Reset until a check mark appears, then click submit.
4.2 MAC Rules

Click on the MAC Rules tab at the top of the Circuit Configuration window.

4.2.1 Select Port for Configuration

Using the pull-down menus, select the slot number and port number of the port for which you wish to configure a MAC Rule. The Slot pull-down menu will only list the DSLAM slots that are occupied by an interface module; empty slots and slots occupied

**NOTE** A reset will not take place unless it is submitted.
by blank plates will not be listed. The slot selected will be detailed in the Device Type and Revision fields. In the following illustration, Port 11 in Slot 2 has been chosen for configuration; Slot 2 contains a SIM2000-24 with firmware revision 2.00.00.

### 4.2.2 Circuit Configuration MAC Rules

Medium Access Control (MAC) ranges are a method of providing OSI Layer 2 identification information for prioritization purposes. Packet priority is assigned based on the source and/or destination MAC address of the packet. Up to four [4] separate MAC Rules may be configured per port.
4.2.2.1 Activate Rule

A MAC Rule will not be applied to the selected port unless it is activated. Use the pull-down menu to select either yes or no. Default is no.

4.2.2.2 MAC Range

Packets containing a source and/or destination MAC address that falls within the configured range will match the MAC portion of the MAC Rule. Default is 00:00:00:00:00:00 - 00:00:00:00:00:00. No packets will match at the default MAC Range setting; you must configure the MAC Range as is appropriate for your individual network.

NOTE You may wish to submit (Section 4.2.3) an added MAC Rule and then review your parameter configurations prior to activation.

4.2.2.2.1 Single MAC Address

Only packets with the specified MAC address, as either their source or destination, will match the MAC address portion of the MAC Rule.
4.2.2.2 MAC Range
Only packets with a source and/or destination MAC address within the specified range will match the MAC address portion of the MAC Rule.

<table>
<thead>
<tr>
<th>MAC Range</th>
<th>Start MAC = End MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:50:ca:00:00:00</td>
<td></td>
</tr>
<tr>
<td>00:50:ca:00:00:00</td>
<td></td>
</tr>
</tbody>
</table>

4.2.2.3 Allow Tag or Untag on Ingress Packets
Use the pull-down menu to select either tag or untag. Tag indicates that ingress packets already matched to the MAC Rule must have a VLAN tag to be further considered; packets without a VLAN tag will be dropped. Untag indicates that ingress packets already matched to the MAC Rule cannot have a VLAN tag to be further considered; packets with a VLAN tag will be dropped. Default is untag.

4.2.2.4 VLAN
For each individual MAC Rule, if you selected tag in Section 4.2.2.3, the VLAN field should specify either an acceptable Single VLAN, or an acceptable VLAN Range, for VLAN tags on ingress packets. If you selected untag, the VLAN field should specify a Single VLAN only if you intend to have a VLAN tag added to packets (Section 4.2.2.5); if you do not intend to have a VLAN tag added to packets, the VLAN field should be left at the 0 - 0 default.

### MAC Rule Settings

<table>
<thead>
<tr>
<th>Address Rule</th>
<th>MAC Range</th>
<th>Allow Tag/Untag on Ingress</th>
<th>VLAN (1-4095)</th>
<th>All VLANs</th>
<th>Priority</th>
<th>Port/Map</th>
<th>Queue</th>
<th>Level (Bytes)</th>
<th>Drop (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. When allow or ingress rule, the port sets or VID CL VLAN mode, otherwise the port sets are all VID CL VLAN.
2. Add a single VLAN tag to the ingress rule when Allow/Tag/Untag on Ingress Rule is not to tag.
3. The VLAN/Map information will be applied to the VLAN priority when Allow/Tag/Ingress Rule is or to tag.

4.2.2.4.1 Single VLAN
If tag was selected in Section 4.2.2.3, only packets with the specified VLAN tag will match the VLAN portion of the MAC Rule. If untag was selected, a Single VLAN should only be specified if the MAC Rule is also configured to add a VLAN tag to packets (Section 4.2.2.5).
4.2.2.4.2 VLAN Range

A VLAN range should only be specified if *tag* was selected in Section 4.2.2.3. Only packets tagged within the specified VLAN range will match the VLAN portion of the MAC Rule. If a VLAN Range is specified, the MAC Rule MUST be configured to allow packets to continue on with the same VLAN tag they came in with (Section 4.2.2.5).

<table>
<thead>
<tr>
<th>Start Tag = End Tag</th>
<th>VLAN Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>untag</em></td>
<td>no VLAN tag</td>
<td>match</td>
<td>have the configured VLAN tag added</td>
<td></td>
</tr>
<tr>
<td></td>
<td>any VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td><em>tag</em></td>
<td>no VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the specified VLAN tag</td>
<td>match</td>
<td>keep the same VLAN tag</td>
<td></td>
</tr>
<tr>
<td></td>
<td>any VLAN tag other than the specified VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

4.2.2.5 Add VLAN Tag to Ingress Packets

Use the pull-down menu to select either *yes* or *no*. Default is *no*.

<table>
<thead>
<tr>
<th>Start Tag &lt; End Tag</th>
<th>VLAN Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>tag</em></td>
<td>no VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>any VLAN tag within the specified range</td>
<td>match</td>
<td>keep the same VLAN tag</td>
<td></td>
</tr>
<tr>
<td></td>
<td>any VLAN tag not in the specified range</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

---

1. When allow tag on ingress pkt, the port acts as 802.1Q VLAN trunk, whereas the port acts as 802.1Q VLAN access.
2. Add a single VLAN tag to the ingress pkt when *Add VLAN to Ingress Pkt* is *yes*.
3. The VLAN MAC address will be applied to the VLAN priority when *Add VLAN to Ingress Pkt* is *yes*. 
4. Add VLAN to Ingress Pkt: *no* or *yes*.
4.2.2.6 Priority
Use the pull-down menu to select a priority value from 0 - 7, where 0 is no priority, 1 is the lowest priority and 7 is the highest priority. Default is 0.
4.2.2.7.1  Fixed (default)
The packet's original priority will automatically be replaced with the MAC Rule Priority (Section 4.2.2.6).

4.2.2.7.2  Max
The packet's original priority will only be replaced with the configured MAC Rule Priority (Section 4.2.2.6) if the packet's original priority is greater than the MAC Rule Priority. E.g. If the MAC Rule Priority has been configured at 4, a packet's original priority will be replaced only if it is greater than 4 (as in 5, 6 or 7).

NOTE  The MAC Rule Fixed/Max parameter does not apply to packets that have come in through an uplink connection; neither will the Fixed/Max configuration come into play if a QoS Backbone VLAN ID (Section 4.3.3.2) has been configured.

4.2.2.8  Ingress and Egress Limits
Ingress Limit and Egress Limit allow traffic-specific, rule-specific, bandwidth limits to be set for each port. Unit of measure is kbps. Default is 0 (no limit).

4.2.2.9  Matching Packets with a MAC Rule
The first step in matching a packet with a MAC Rule is matching the destination and/or source MAC address. Once it has been determined that a packet's destination and/or source MAC address matches the configured single MAC or MAC range of a MAC Rule, it must then match all other criteria for that rule as well, or the packet will be dropped. If a packet's destination and/or source MAC address does not match the single MAC or MAC range of a MAC Rule, the packet will be passed on for an attempted match with the next rule in line.

NOTE  If a packet's destination and/or source MAC address matches the single MAC or MAC range of a MAC Rule but fails to match one or more of the other criteria for that rule, it will be dropped; it will not continue on to the next rule.

4.2.2.9.1  Packets with a VLAN Tag
When Allow Tag/Untag on Ingress Pkt. is set to tag (Section 4.2.2.3), a tagged packet with a MAC address and VLAN that match the configurations of a MAC Rule will be deemed a match with that rule and no further attempts will be made to match that packet with any other QoS Rules. Additionally, once a packet has been matched with a MAC Rule, it will conform to the priority and bandwidth limits as configured for that rule.
4.2.2.9.2 Packets without a VLAN Tag
When Allow Tag/Untag on Ingress Pkt. is set to untag (Section 4.2.2.3), an untagged packet with a MAC address that matches the configurations of a MAC Rule will be deemed a match with that rule and no further attempts will be made to match that packet with any other QoS Rules. Additionally, once a packet has been matched with a MAC Rule, it will conform to the VLAN and priority configurations, as well as bandwidth limits, as configured for that rule.

4.2.3 Submit Circuit MAC Rules
Once all parameters in the Circuit Configuration MAC Rules window have been configured as desired, click the submit button at the bottom of the window. Any configurations that are not submitted will be discarded. If any accidental or undesirable changes have been made, exit the screen without clicking submit and the changes will be discarded. If any accidental or undesirable changes have already been submitted, simply make the desired adjustments and then resubmit the rule.
4.2.4 Reset Circuit MAC Rules

Resetting a port's MAC Rules will return ALL of that port's MAC Rules to their original default settings. Click the box to the left of the Reset until a check mark appears, then click submit.

NOTE A reset will not take place unless it is submitted.
4.3 VLAN Rules

Click on the VLAN Rules tab at the top of the Circuit Configuration window.

4.3.1 Select Port for Configuration

Using the pull-down menus, select the slot number and port number of the port for which you wish to configure a VLAN Rule. The Slot pull-down menu will only list the DSLAM slots that are occupied by an interface module; empty slots and slots occupied by blank plates will not be listed. The slot selected will be detailed in the Device Type and Revision fields. In the following illustration, Port 11 in Slot 2 has been chosen for configuration; Slot 2 contains a SIM2000-24 with firmware revision 2.00.00.
4.3.2 Circuit Configuration VLAN Rules

Virtual Local Area Network (VLAN) tag ranges are a method of providing OSI Layer 2 identification information for prioritization purposes. Packet priority is assigned based on the packet's VLAN tag. Up to ten [10] separate VLAN Rules may be configured per port.

Default on all ports is for one VLAN Rule to be activated with all parameters at default settings (as shown on the following page); no Diffserv, IP Range or MAC Rules are activated by default. An activated VLAN Rule that has been left at default settings will allow all untagged packets to be forwarded (with no priority) and, if no additional QoS Rules are activated, all tagged packets will be dropped.
4.3.2.1 Activate Rule

A VLAN Rule will not be applied to the selected port unless it is activated. Use the pull-down menu to select either yes or no. Default is no.

<table>
<thead>
<tr>
<th>VLAN Rules Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

4.3.2.2 Allow Tag or Untag on Ingress Packets

Use the pull-down menu to select either tag or untag. Tag indicates that only ingress packets with a VLAN tag will be considered; all ingress packets without a VLAN tag will be passed on for an attempted match with the next VLAN Rule in line. Untag indicates that only ingress packets without a VLAN tag will be considered; all ingress packets with a VLAN tag will be passed on for an attempted match with the next VLAN Rule in line. Default is untag.

4.3.2.3 VLAN

For each individual VLAN Rule, if you selected tag in Section 4.3.2.2, the VLAN field should specify either an acceptable Single VLAN, or an acceptable VLAN Range, for VLAN tags on ingress packets. If you selected untag, the VLAN field should specify a Single VLAN only if you intend to have a VLAN tag added to

**NOTE**

You may wish to submit (Section 4.3.4) an added VLAN Rule and then review your parameter configurations prior to activation.

**NOTE**

No more than one VLAN Rule per port should be configured to allow packets without a VLAN tag (untag); any untagged packets that have not already been matched to a Diffserv, IP Range or MAC Rule will automatically be matched with the FIRST VLAN Rule that allows untagged packets. Therefore, any subsequent VLAN Rules allowing untagged packets will not be utilized.
packets (Section 4.3.2.4); if you do not intend to have a VLAN tag added to packets, the VLAN field should be left at the 0 - 0 default.

4.3.2.3.1 Single VLAN
If tag was selected in Section 4.3.2.2, only packets with the specified VLAN tag will match the VLAN Rule. If untag was selected, a Single VLAN should only be specified if the VLAN Rule is configured to add a VLAN tag to packets (Section 4.3.2.4).

4.3.2.3.2 VLAN Range
A VLAN range should only be specified if tag was selected in Section 4.3.2.2. Only packets tagged within the specified VLAN range will match the VLAN Rule. If a VLAN Range is specified, the VLAN Rule MUST be configured to allow packets to continue on with the same VLAN tag they came in with (Section 4.3.2.4).
4.3.2.4 Add VLAN Tag to Ingress Packets

Use the pull-down menu to select either yes or no. Default is no.

For a packet that has already been matched to a VLAN Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the VLAN Rule must be configured with a single VLAN (Section 4.3.2.3.1) and a VLAN tag with the specified value will be added to the packet</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>the packet will continue on without a VLAN tag</td>
</tr>
<tr>
<td>tag</td>
<td>yes*</td>
<td>the packet will continue on with the same VLAN tag it had at ingress</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 4.2.2.2).

4.3.2.5 Priority

Use the pull-down menu to select a priority value from 0 - 7, where 0 is no priority, 1 is the lowest priority and 7 is the highest priority. Default is 0.
4.3.2.6 Fixed or Maximum Priority

The Fixed/Max field dictates the action to be taken with the configured Priority (Section 4.3.2.5) of a tagged packet that has come in through a subscriber connection and has already been matched to a VLAN Rule. Use the pull-down menu to select either fixed or max. Default is fixed.

### 4.3.2.6.1 Fixed (default)

The packet's original priority will automatically be replaced with the VLAN Rule Priority (Section 4.3.2.5).

### 4.3.2.6.2 Max

The packet's original priority will only be replaced with the configured VLAN Rule Priority (Section 4.3.2.5) if the packet's original priority is greater than...
the VLAN Rule Priority. E.g. If the VLAN Rule Priority has been configured at 4, a packet's original priority will be replaced only if it is greater than 4 (as in 5, 6 or 7).

**NOTE** The VLAN Rule Fixed/Max parameter does not apply to packets that have come in through an uplink connection; neither will the Fixed/Max configuration come into play if a QoS Backbone VLAN ID (Section 4.3.3.2) has been configured.

### 4.3.2.7 Ingress and Egress Limits
Ingress Limit and Egress Limit allow traffic-specific, rule-specific, bandwidth limits to be set for each port. Unit of measure is kbps. Default is 0 (no limit).

### 4.3.2.8 Matching Packets with a VLAN Rule
The first step in matching a packet with a VLAN Rule requires a determination of whether or not the packet has a VLAN tag. If the VLAN Rule has been configured to allow only tagged packets, then all untagged packets will be passed on for an attempted match with the next VLAN Rule in line, as will any tagged packets with a VLAN tag falling outside of the configured range (Section 4.3.2.3). If the VLAN Rule has been configured to allow only untagged packets, then all tagged packets will be passed on for an attempted match with the next VLAN Rule in line.

#### 4.3.2.8.1 Packets with a VLAN Tag
When Allow Tag/Untag on Ingress Pkt. is set to *tag* (Section 4.3.2.2), then any packet having a VLAN tag within the configured range (Section 4.3.2.3) will be deemed a match with that VLAN Rule and no further attempts will be made to match that packet with any other VLAN Rules. Additionally, once a packet has been matched with a VLAN Rule, it will conform to the priority configuration and bandwidth limits of that rule.

---

*If a QoS Rule Backbone VLAN has been configured, then the Backbone VLAN will be taken into consideration along with the standard VLAN in determining whether a packet matches a VLAN Rule. Refer to Section 4.3.3.2 for further information regarding Backbone VLAN.*
4.3.2.8.2 Packets without a VLAN Tag
When Allow Tag/Untag on Ingress Pkt. is set to untag (Section 4.3.2.2) then all packets without a VLAN tag will be deemed a match with that VLAN Rule and no further attempts will be made to match those packets with any other VLAN Rules. Additionally, once a packet has been matched with a VLAN Rule, it will conform to the priority configurations and bandwidth limits of that rule.

4.3.3 Backbone and Flood
Backbone Ethertype, Backbone VLAN Identification (ID) and Flood, as configured here, apply to ALL QoS Rules: DiffServ Rules, IP Range Rules, MAC Rules and VLAN Rules. These parameters cannot be applied on their own; there must be at least one QoS rule activated. To this end, one VLAN Rule is activated as a QoS default; refer to Section 4.3.2 for a description.

4.3.3.1 Backbone Ethertype
Backbone Ethertype is a two-byte code indicating packet type. Use the pull-down menu to select either 8100 or 9100; selection should be based on the type of packets supported by your router. Default is 8100.
4.3.3.2 Backbone VLAN ID

Used in conjunction with standard VLAN tags, a single Backbone VLAN tag will become the primary identifier, allowing a router with backbone capabilities to make smarter decisions in directing traffic to the proper network. Once a packet has reached the proper network, its standard VLAN tags will direct it to the appropriate port. To configure Backbone VLAN ID, enter a single VLAN tag value between 0 and 4085. Default is 0, indicating that the Backbone VLAN function is not in use.

For a packet that has already been matched with a QoS Rule:

<table>
<thead>
<tr>
<th>ingress packets from the</th>
<th>with</th>
<th>will be _____ when Backbone VLAN IS configured</th>
<th>will be _____ when Backbone VLAN IS NOT configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>subscriber (WAN)</td>
<td>both Backbone VLAN and standard VLAN tags</td>
<td>DROPPED regardless of whether the packet's Backbone VLAN tag is in accordance with current configurations.</td>
<td>DROPPED</td>
</tr>
<tr>
<td></td>
<td>standard VLAN tags only</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched. A Backbone VLAN tag with the QoS Rule Priority* will be added prior to transmission (the standard VLAN tag will maintain the Priority configuration the packet had at ingress).</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched.</td>
</tr>
<tr>
<td></td>
<td>no VLAN tags: neither Backbone VLAN nor standard VLAN</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched. A Backbone VLAN tag and a standard VLAN tag, both with the QoS Rule Priority*, will be added to the packet prior to transmission.</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched. A standard VLAN tag with the QoS Rule Priority will be added prior to transmission.</td>
</tr>
<tr>
<td>uplink</td>
<td>both Backbone VLAN and standard VLAN tags</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched as long as the packet's Backbone VLAN tag matches the QoS Rule's Backbone VLAN configuration. The Backbone VLAN tag will be stripped prior to packet transmission. The packet will be DROPPED if its Backbone VLAN tag does not match the QoS Rule's Backbone VLAN configuration.</td>
<td>DROPPED</td>
</tr>
<tr>
<td></td>
<td>standard VLAN tags only</td>
<td>DROPPED</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched.</td>
</tr>
</tbody>
</table>
4.3.3.3 Flood

Flood refers to the method in which interface modules handle unknown unicasts (traffic directed to a single MAC address), broadcasts (traffic directed to all MAC addresses) and multicasts (traffic directed to multiple MAC addresses) for each port. Use the pull-down menu to select either *Upl* (uplink) or *Vln* (VLAN: access ports). Default is *Upl*.

4.3.3.3.1 Uplink (default)

Unknown unicast, broadcast and multicast traffic will be flooded to the DSLAM uplink interface ports, preventing communication between interface ports without the intervention of an upstream device such as a router. If communication between interface ports is desired, the upstream device must be properly configured to allow it.

4.3.3.3.2 VLAN

Unknown unicast, broadcast and multicast traffic will be flooded to both DSLAM access ports (within the sender's VLAN range) and the uplink interface ports.

4.3.4 Submit Circuit VLAN Rules

Once all parameters in the Circuit Configuration VLAN Rules window have been configured as desired, click the *submit* button at the bottom of the window. Any configurations that are not submitted will be discarded. If any accidental or undesirable changes have been made, exit the screen without clicking *submit* and the changes will be discarded. If any accidental or undesirable changes have already been submitted, simply make the desired adjustments and then resubmit the rule.

---

**NOTE**
A Backbone VLAN tag cannot be used independently; standard VLAN tags must also be configured. Additionally, the DSLAM uplink connection must run through a router in order for a Backbone VLAN tag to function.

---

*The Fixed/Max configuration of a QoS Rule will not come into play when a Backbone VLAN ID has been configured.*

A Backbone VLAN tag cannot be used independently; standard VLAN tags must also be configured. Additionally, the DSLAM uplink connection must run through a router in order for a Backbone VLAN tag to function.
4.3.5 Reset Circuit VLAN Rules

Resetting a port's VLAN Rules will return ALL of that port's VLAN Rules to their original default settings. Click the box to the left of the Reset until a check mark appears, then click submit.

NOTE A reset will not take place unless it is submitted.
5.0 GLOBAL QoS RULES

From the NMS main window, click the "Global Set" button on the left hand side of the screen to get to the Global Set window.

5.1 Global DSCP & IP Rules

Click on the Global DSCP & IP Rules tab at the top of the Global Set window.
5.1.1 Select Slot(s) and Port(s) for Configuration

5.1.1.1 Slot
Using the pull-down menu, select the slot number of the interface module for which you wish to configure a Diffserv or IP Range Rule. The Slot pull-down menu will only list the DSLAM slots that are occupied by an interface module; empty slots and slots occupied by blank plates will not be listed. The slot selected will be detailed in the Device Type and Revision fields. In the following illustration, there are interface modules in slots 1 and 2; Slot 2 has been selected and contains a SIM2000-24 with firmware revision 2.00.00.

<table>
<thead>
<tr>
<th>Slot</th>
<th>Device Type</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>SIM2000-24</td>
<td>2.00.00</td>
</tr>
</tbody>
</table>

**NOTE** There is no Slot selection field in the NMS Global Set window for Net to Net's Micro and Mini DSLAMs, only a Port selection field.

5.1.1.2 Add Slot(s)
After clicking the initial slot number in the Slot pull-down menu, hold down the "Ctrl" key on your keyboard to click (select) additional slot numbers (IP DSLAMs only). The additional slot numbers will appear in the field under Add Slot(s).

**NOTE** When configuring multiple interface modules at one time, all chosen modules must be of the same model type; NMS will not allow selection of different interface module models. Firmware versions may vary amongst the chosen slots however, as long as the models are the same.

As illustrated here (and in Section 5.1.1.1), Slot 2 was the first slot selected; Slot 1 has been added. Since the interface module in Slot 2 is a SIM2000-24 (as illustrated in Section 5.1.1.1) the interface module in Slot 1 must also be SIM2000-24.
5.1.1.3 Add Port(s)
Ports may be selected singly, in multiples, or all at once. To select a single port, click on the number of the port you wish to configure. Hold down the "Ctrl" key on your keyboard to click (select) additional port numbers. Scroll down the Add Port(s) menu, if necessary, to access all of the port numbers you wish to select. To select ALL ports, click All. The port selections you make will apply to all of the previously selected interface modules (Section 5.1.1.1 and 5.1.1.2).

In this illustration ALL ports have been selected. As applied to the example in Section 5.1.1.2, a configured Global Diffserv and/or IP Range Rule will be applied to ALL ports in both Slot 1 and Slot 2.

5.1.2 Global Configuration Diffserv Rules
A Differentiated Services Code Point (DSCP) provides OSI Layer 3 identification information within a packet's IP header for the purpose of determining packet type. Up to four [4] separate Differentiated Services (Diffserv) Rules may be configured per port.

**NOTE** Ethertype 0x800 IP packets are the only type of packets that can be matched with Diffserv Rules.

5.1.2.1 Add, Delete or Do Not Set
Global Diffserv Rules can be added or deleted, they cannot be modified. If you wish to change a rule that has already been added, you will need to delete the rule and then add a new rule with the desired change(s).

5.1.2.1.1 Add
Add indicates that you wish to add a Diffserv Rule to the selected slot(s)/port(s).
5.1.2.1.2 Delete

Delete indicates that you wish to remove a Diffserv Rule that was previously applied to the selected slot(s)/port(s). In order to successfully delete a Global Diffserv Rule, the configurations for EVERY FIELD must exactly match that of the rule you wish to delete.

NOTE If you are unsure of one or more of the settings for a rule you wish to delete, you may view all of that rule’s configured parameters by returning to the main window, clicking on the depicted LED for one of the ports to which the rule is currently applied, and then clicking on the DSCP & IP Rules tab at the top of the Circuit Configuration window; all Diffserv and IP Range Rules associated with that port will be listed along with their individual parameter settings.

5.1.2.1.3 Do Not Set (default)

No Set simply maintains the status quo of a Diffserv or IP Range Rule for the selected slot(s)/port(s). Clicking submit at the bottom of the DSCP & IP Rules window applies to both Diffserv AND IP Range Rules, thus, if you wish to set only one of the two, the one you do NOT wish to set should be configured as No Set. I.e., if you wish to add or delete a Diffserv Rule without also adding or deleting an IP Range Rule, then the Global IP Range Rule should be configured as No Set; if you wish to add or delete an IP Range Rule without also adding or deleting a Diffserv Rule, then the Global Diffserv Rule should be configured as No Set.

5.1.2.2 Activate Rule

A Global Diffserv Rule will not be applied to the selected slot(s)/port(s) unless it is activated. Use the pull-down menu to select either yes or no. Default is no.

5.1.2.3 Differentiated Services (DS) Value and Mask

5.1.2.3.1 DS Value

The DS Value of a packet is a hexadecimal value calculated from the upper six [6] bits of an eight [8] bit field in the packet’s IP header (the remaining two [2] bits are unused) known as the Differentiated Services Code Point (DSCP). It is one of several methods used to determine packet type. Configuring a DS Value requires knowledge of your (desired) network traffic and, as such, a default value is not applicable (indicated as 00).

NOTE Though it is only the upper six bits of the eight bit field in a packet’s IP header that comprise the DSCP, DS Value calculations require that all eight bits be configured nonetheless.
5.1.2.3 DS Mask
The DS Mask is a hexadecimal value that indicates which of the DSCP's upper six [6] bits will be utilized in considering a packet's DSCP type. Default is FC, indicating that ALL of the DSCP's upper six bits will be used in calculating the packet's DS Value.

How It Works:
A "logical bit-wise AND" is performed between a packet's DSCP and the DS Mask value of the Diffserv Rule. The result must equal the DS Value configured for that Diffserv Rule in order for the packet to match the DS Value portion of that rule.

5.1.2.4 Allow Tag or Untag on Ingress Packets
Use the pull-down menu to select either tag or untag. Tag indicates that ingress packets already matched to the Diffserv Rule must have a VLAN tag to be further considered; packets without a VLAN tag will be dropped. Untag indicates that ingress packets already matched to the Diffserv Rule cannot have a VLAN tag to be further considered; packets with a VLAN tag will be dropped. Default is untag.

5.1.2.5 VLAN
For each Global Diffserv Rule, if you selected tag in Section 5.1.2.4, the VLAN field should specify either an acceptable Single VLAN, or an acceptable VLAN Range, for VLAN tags on ingress packets. If you selected untag, the VLAN field should specify a Single VLAN only if you intend to have a VLAN tag added to packets (Section 5.1.2.6); if you do not intend to have a VLAN tag added to packets, the VLAN field should be left at the 0 - 0 default.

5.1.2.5.1 Single VLAN
If tag was selected in Section 5.1.2.4, only packets with the specified VLAN tag will match the VLAN portion of the Diffserv Rule. If untag was selected, a Single VLAN should only be specified if the Diffserv Rule is also configured to add a VLAN tag to packets (Section 5.1.2.6).

For a packet that has already been matched to a Diffserv Rule:

<table>
<thead>
<tr>
<th>VLAN (1-4085)</th>
<th>Start Tag = End Tag</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>no VLAN tag</td>
<td>match</td>
<td>have the configured VLAN tag added</td>
</tr>
<tr>
<td></td>
<td>any VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
</tr>
</tbody>
</table>

QoS Management User Guide 210-0000055 rev02
5.1.2.5.2 VLAN Range
A VLAN range should only be specified if *tag* was selected in Section 5.1.2.4. Only packets tagged within the specified VLAN range will match the VLAN portion of the Diffserv Rule. If a VLAN Range is specified, the Diffserv Rule MUST be configured to allow packets to continue on with the same VLAN tag they came in with (Section 5.1.2.6).

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>tag</em></td>
<td>no VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
</tr>
<tr>
<td>the specified VLAN tag</td>
<td>match</td>
<td>keep the same VLAN tag</td>
<td></td>
</tr>
<tr>
<td>any VLAN tag other than the specified VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

5.1.2.6 Add VLAN Tag to Ingress Packets
Use the pull-down menu to select either *yes* or *no*. Default is *no*.

For a packet that has already been matched to a Diffserv Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>tag</em></td>
<td>no VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
</tr>
<tr>
<td>any VLAN tag within the specified range</td>
<td>match</td>
<td>keep the same VLAN tag</td>
<td></td>
</tr>
<tr>
<td>any VLAN tag not in the specified range</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as *yes* when tagged packets are allowed (Section 5.1.2.4).*
5.1.2.7 Priority
Use the pull-down menu to select a priority value from 0 - 7, where 0 is no priority, 1 is the lowest priority and 7 is the highest priority. Default is 0.

For a packet that has come in through a subscriber connection and has already been matched to a Diffserv Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN To Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the Diffserv Rule Priority will be added to the packet as part of the VLAN tag and will be applied to the packet both within the DSLAM and at egress</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>the packet will follow the Diffserv Rule Priority within the DSLAM only; it will not be added to the packet at egress</td>
</tr>
<tr>
<td>tag</td>
<td>yes*</td>
<td>Priority will be applied according to the Diffserv Rule Fixed/Max configuration (Section 5.1.2.8)</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 5.1.2.4).

**NOTE** Diffserv Rule Priority configurations do not apply to packets that have come in through an uplink connection; packets coming from an uplink connection will retain their original priority.

5.1.2.8 Fixed or Maximum Priority
The Fixed/Max field dictates the action to be taken with the configured Priority (Section 5.1.2.7) of a tagged packet that has come in through a subscriber connection and has already been matched to a Diffserv Rule. Use the pull-down menu to select either fixed or max. Default is fixed.

5.1.2.8.1 Fixed (default)
The packet's original priority will automatically be replaced with the Diffserv Rule Priority (Section 5.1.2.7).

5.1.2.8.2 Max
The packet's original priority will only be replaced with the configured Diffserv Rule Priority (Section 5.1.2.7) if the packet's original priority is greater than the Diffserv Rule Priority. E.g. If the Diffserv Rule Priority has been configured at 4, a packet's original priority will be replaced only if it is greater than 4 (as in 5, 6 or 7).
5.1.2.9  Ingress and Egress Limits

Ingress Limit and Egress Limit allow traffic-specific, rule-specific, bandwidth limits to be set for each port. Unit of measure is kbps. Default is 0 (no limit).

5.1.2.10  Matching Packets with a Diffserv Rule

The first step in matching a packet with a Diffserv Rule is matching the DS Value. Once it has been determined that a packet matches the DS Value of a Diffserv Rule, that packet must then match all other criteria for that rule as well, or it will be dropped. If a packet does not match the DS Value of a rule, it will be passed on for an attempted match with the next rule in line.

NOTE  If a packet matches a Diffserv Rule’s DS Value but fails to match one or more of the other criteria for that rule, it will be dropped; it will not continue on to the next rule.

5.1.2.10.1  Packets with a VLAN Tag

When Allow Tag/Untag on Ingress Pkt. is set to tag (Section 5.1.2.4), a tagged packet with a DS Value and VLAN that match the configurations of a Diffserv Rule will be deemed a match with that rule and no further attempts will be made to match that packet with any other QoS Rules. Additionally, once a packet has been matched with a Diffserv Rule, it will conform to the priority and bandwidth limits as configured for that rule.

5.1.2.10.2  Packets without a VLAN Tag

When Allow Tag/Untag on Ingress Pkt. is set to untag (Section 5.1.2.4), an untagged packet with a DS Value that matches the configurations of a Diffserv Rule will be deemed a match with that rule and no further attempts will be made to match that packet with any other QoS Rules. Additionally, once a packet has been matched with a Diffserv Rule, it will conform to the VLAN and priority configurations, as well as bandwidth limits, as configured for that rule.

NOTE  The Diffserv Fixed/Max parameter does not apply to packets that have come in through an uplink connection; neither will the Fixed/Max configuration come into play if a QoS Backbone VLAN ID (Section 5.3.3.2) has been configured.

NOTE  If a packet matches a Diffserv Rule’s DS Value but fails to match one or more of the other criteria for that rule, it will be dropped; it will not continue on to the next rule.

*If a QoS Rule Backbone VLAN has been configured, then the Backbone VLAN will be taken into consideration along with the standard VLAN in determining whether a packet matches a Diffserv Rule. Refer to Section 5.3.3.2 for further information regarding Backbone VLAN.
5.1.3 Global Configuration IP Range Rules

Internet Protocol (IP) address ranges are a method of providing OSI Layer 3 identification information for prioritization purposes. Packet priority is assigned based on the source and/or destination IP address of the packet. Up to four [4] separate IP address Rules may be configured per port.

**NOTE** Ethertype 0x800 and 0x806 IP packets are the only type of packets that can be matched with IP Range Rules.

5.1.3.1 Add, Delete or Do Not Set

Global IP Range Rules can be added or deleted, they cannot be modified. If you wish to change a rule that has already been added, you will need to delete the rule and then add a new rule with the desired change(s).

5.1.3.1.1 Add

Add indicates that you wish to add an IP Range Rule to the selected slot (s)/port(s).
5.1.3.1.2 Delete

delete indicates that you wish to remove an IP Range Rule that was previously applied to the selected slot(s)/port(s). In order to successfully delete a Global IP Range Rule, the configurations for EVERY FIELD must exactly match that of the rule you wish to delete.

5.1.3.1.3 Do Not Set (default)

No Set simply maintains the status quo of a Diffserv or IP Range Rule for the selected slot(s)/port(s). Clicking submit at the bottom of the DSCP & IP Rules window applies to both Diffserv AND IP Range Rules, thus, if you wish to set only one of the two, the one you do NOT wish to set should be configured as No Set. I.e., if you wish to add or delete a Diffserv Rule without also adding or deleting an IP Range Rule, then the Global IP Range Rule should be configured as No Set; if you wish to add or delete an IP Range Rule without also adding or deleting a Diffserv Rule, then the Global Diffserv Rule should be configured as No Set.

5.1.3.2 Activate Rule

A Global IP Range Rule will not be applied to the selected slot(s)/port(s) unless it is activated. Use the pull-down menu to select either yes or no. Default is no.

5.1.3.3 IP Range

Packets containing a source and/or destination IP address that falls within the configured range will match the IP portion of the IP Range Rule. Default is 0.0.0.0 - 0.0.0.0. No packets will match at the default IP Range setting; you must configure the IP Range as is appropriate for your individual network.

5.1.3.3.1 Single IP Address

Only packets with the specified IP address, as either their source or destination, will match the IP address portion of the IP Range Rule.
5.1.3.3.2 IP Range
Only packets with a source and/or destination IP address within the specified range will match the IP address portion of the IP Range Rule.

5.1.3.3 Full IP Range
All packets will match the IP portion of the IP Range Rule.

5.1.3.4 Allow Tag or Untag on Ingress Packets
Use the pull-down menu to select either tag or untag. Tag indicates that ingress packets already matched to the IP Range Rule must have a VLAN tag to be further considered; packets without a VLAN tag will be dropped. UnTag indicates that ingress packets already matched to the IP Range Rule cannot have a VLAN tag to be further considered; packets with a VLAN tag will be dropped. Default is untag.

5.1.3.5 VLAN
For each Global IP Range Rule, if you selected tag in Section 5.1.3.4, the VLAN field should specify either an acceptable Single VLAN, or an acceptable VLAN Range, for VLAN tags on ingress packets. If you selected untag, the VLAN field should specify a Single VLAN only if you intend to have a VLAN tag added to packets (Section 5.1.3.6); if you do not intend to have a VLAN tag added to packets, the VLAN field should be left at the 0 - 0 default.

5.1.3.5.1 Single VLAN
If tag was selected in Section 5.1.3.4, only packets with the specified VLAN tag will match the VLAN portion of the IP Range Rule. If untag was selected, a Single VLAN should only be specified if the IP Range Rule is also configured to add a VLAN tag to packets (Section 5.1.3.6).
5.1.3.5.2 VLAN Range

A VLAN range should only be specified if *tag* was selected in Section 5.1.3.4. Only packets tagged within the specified VLAN range will match the VLAN portion of the IP Range Rule. If a VLAN range is specified, the IP Range Rule **MUST** be configured to allow packets to continue on with the same VLAN tag they came in with (Section 5.1.3.6).

For a packet that has already been matched to an IP Range Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>untag</em></td>
<td>no VLAN tag</td>
<td>match</td>
<td>have the configured VLAN tag added</td>
</tr>
<tr>
<td></td>
<td>any VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
</tr>
<tr>
<td><em>tag</em></td>
<td>no VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>the specified VLAN tag</td>
<td>match</td>
<td>keep the same VLAN tag</td>
</tr>
<tr>
<td></td>
<td>any VLAN tag other than the specified VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
</tr>
</tbody>
</table>

5.1.3.6 Add VLAN Tag to Ingress Packets

Use the pull-down menu to select either *yes* or *no*. Default is *no*. 

![Diagram of VLAN range configuration](image)

*Note:* When *untag* is selected in ingress, the port must be in the VLAN range, otherwise the port is in the VLAN range.
For a packet that has already been matched to an IP Range Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the IP Range Rule must be configured with a single VLAN (Section 5.1.3.5.1) and a VLAN tag with the specified value will be added to the packet</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>the packet will continue on without a VLAN tag</td>
</tr>
<tr>
<td>tag</td>
<td>yes</td>
<td>the packet will continue on with the same VLAN tag it had at ingress</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 5.1.3.4).

### 5.1.3.7 Priority

Use the pull-down menu to select a priority value from 0 - 7, where 0 is no priority, 1 is the lowest priority and 7 is the highest priority. Default is 0.

![Global Configuration IP Range Rules](image)

For a packet that has come in through a subscriber connection and has already been matched to an IP Range Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Packet is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the IP Range Rule Priority will be added to the packet as part of the VLAN tag and will be applied to the packet both within the DSLAM and at egress</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>the packet will follow the IP Range Rule Priority within the DSLAM only; it will not be added to the packet at egress</td>
</tr>
<tr>
<td>tag</td>
<td>yes*</td>
<td>Priority will be applied according to the IP Range Rule Fixed/Max configuration (Section 5.1.3.8)</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 5.1.3.4).

**NOTE** IP Range Rule Priority configurations do not apply to packets that have come in through an uplink connection; packets coming from an uplink connection will retain their original priority.

### 5.1.3.8 Fixed or Maximum Priority

The Fixed/Max field dictates the action to be taken with the configured Priority (Section 5.1.3.7) of a tagged packet that has come in through a subscriber connection and has already been matched to an IP Range Rule. Use the pull-down menu to select either fixed or max. Default is fixed.
5.1.3.8.1 Fixed (default)
The packet's original priority will automatically be replaced with the IP Range Rule Priority (Section 5.1.3.7).

5.1.3.8.2 Max
The packet's original priority will only be replaced with the configured IP Range Rule Priority (Section 5.1.3.7) if the packet's original priority is greater than the IP Range Rule Priority. E.g. If the IP Range Rule Priority has been configured at 4, a packet's original priority will be replaced only if it is greater than 4 (as in 5, 6 or 7).

**NOTE** The IP Range Rule Fixed/Max parameter does not apply to packets that have come in through an uplink connection; neither will the Fixed/Max configuration come into play if a QoS Backbone VLAN ID (Section 5.3.3.2) has been configured.

5.1.3.9 Ingress and Egress Limits
Ingress Limit and Egress Limit allow traffic-specific, rule-specific, bandwidth limits to be set for each port. Unit of measure is kbps. Default is 0 (no limit).

5.1.3.10 Matching Packets with an IP Range Rule
The first step in matching a packet with an IP Range Rule is matching the destination and/or source IP address. Once it has been determined that a packet's destination and/or source IP address matches the configured Single IP or IP Range of an IP Range Rule, it must then match all other criteria for that rule as well, or the packet will be dropped. If a packet's destination and/or source IP address does not match the Single IP or IP Range of an IP Range Rule, the packet will be passed on for an attempted match with the next rule in line.

**NOTE** If a packet's destination and/or source IP address matches the Single IP or IP Range of an IP Range Rule but fails to match one or more of the other criteria for that rule, it will be dropped; it will not continue on to the next rule.

5.1.3.10.1 Packets with a VLAN Tag
When Allow Tag/Untag on Ingress Pkt. is set to *tag* (Section 5.1.3.4), a tagged packet with an IP address and VLAN that match the configurations of an IP Range Rule will be deemed a match with that rule and no further attempts will be made to match the packet with any other QoS Rules. Additionally, once a packet has been matched with an IP Range Rule, it will conform to the priority and bandwidth limits as configured for that rule.
5.1.3.10.2 Packets without a VLAN Tag
When Allow Tag/Untag on Ingress Pkt. is set to untag (Section 5.1.3.4), an untagged packet with an IP address that matches the configurations of an IP Range Rule will be deemed a match with that rule and no further attempts will be made to match that packet with any other QoS Rules. Additionally, once a packet has been matched with an IP Range Rule, it will conform to the VLAN and priority configurations, as well as bandwidth limits, as configured for that rule.

*If a QoS Rule Backbone VLAN has been configured, then the Backbone VLAN will be taken into consideration along with the standard VLAN in determining whether a packet matches an IP Range Rule. Refer to Section 5.3.3.2 for further information regarding Backbone VLAN.

5.1.4 Submit Global Diffserv & IP Range Rules
Once all parameters in the Global Set DSCP & IP Rules window have been configured as desired, click the submit button at the bottom of the window. Any configurations that are not submitted will be discarded. If any accidental or undesirable changes have been made, exit the screen without clicking submit and the changes will be discarded. If any accidental or undesirable changes have already been submitted, you must delete the affected rule and then create a new rule with the desired settings; refer to Section 5.1.2.1.
5.1.5 Reset Global Diffserv & IP Range Rules
Resetting Diffserv and IP Range Rules will return ALL Diffserv AND IP Range Rules of the selected slot(s)/port(s) to their original default settings; Diffserv and IP Range Rules cannot be reset individually. Click the box to the left of the Reset until a check mark appears, then click submit.

NOTE A reset will not take place unless it is submitted.

5.2 Global MAC Rules
Click on the Global MAC Rules tab at the top of the Global Set window.
5.2.1 Select Slot(s) and Port(s) for Configuration

5.2.1.1 Slot
Using the pull-down menu, select the slot number of the interface module for which you wish to configure a MAC Rule. The Slot pull-down menu will only list the DSLAM slots that are occupied by an interface module; empty slots and slots occupied by blank plates will not be listed. The slot selected will be detailed in the Device Type and Revision fields. In the following illustration, there are interface modules in slots 1 and 2; Slot 2 has been selected and contains a SIM2000-24 with firmware revision 2.00.00.
5.2.1.2 Add Slot(s)
After clicking the initial slot number in the Slot pull-down menu, hold down the "Ctrl" key on your keyboard to click (select) additional slot numbers (IP DSLAMs only). The additional slot numbers will appear in the field under Add Slot(s).

NOTE When configuring multiple interface modules at one time, all chosen modules must be of the same model type; NMS will not allow selection of different interface module models. Firmware versions may vary amongst the chosen slots however, as long as the models are the same.

As illustrated here (and in Section 5.2.1.1), Slot 2 was the first slot selected; Slot 1 has been "added". Since the interface module in Slot 2 is a SIM2000-24 (as illustrated in Section 5.2.1.1) the interface module in Slot 1 must also be a SIM2000-24.

5.2.1.3 Add Port(s)
Ports may be selected singly, in multiples, or all at once. To select a single port, click on the number of the port you wish to configure. Hold down the "Ctrl" key on your keyboard to click (select) additional port numbers. Scroll down the Add Port(s) menu, if necessary, to access all of the port numbers you wish to select. To select ALL ports, click All. The port selections you make will apply to all of the previously selected interface modules (Sections 5.2.1.1 and 5.2.1.2).

In this illustration ALL ports have been selected. As applied to the example in Section 5.2.1.1, the configured Global MAC Rule(s) will be applied to ALL ports in both Slot 1 and Slot 2.

5.2.2 Global Configuration MAC Rules
Medium Access Control (MAC) ranges are a method of providing OSI Layer 2 identification information for prioritization purposes. Packet priority is assigned based on the source and/or destination MAC address of the packet. Up to four [4] separate MAC Rules may be configured per port.
Global MAC Rules can be added or deleted, they cannot be modified. If you wish to change a rule that has already been added, you will need to delete the rule and then add a new rule with the desired change(s).

5.2.2.1.1 Add

"Add" indicates that you wish to add a MAC Rule to the selected slot(s)/port(s).

5.2.2.1.2 Delete

"Delete" indicates that you wish to remove a MAC Rule that was previously applied to the selected slot(s)/port(s). In order to successfully delete a Global MAC Rule, the configurations for EVERY FIELD must exactly match that of the rule you wish to delete.

**NOTE**
If you are unsure of one or more of the settings for a rule you wish to delete, you may view all of that rule’s configured parameters by returning to the main window, clicking on the depicted LED for one of the ports to which the rule is currently applied, and then clicking on the MAC Rules tab at the top of the Circuit Configuration window; all MAC Rules associated with that port will be listed along with their individual parameter settings.

5.2.2.1.3 Do Not Set (default)

"Do Not Set" simply maintains the status quo of a Global MAC Rule: as the default setting, it ensures that a Global MAC Rule will not be added to, or deleted from, any slot(s)/port(s) without deliberate specification.
5.2.2.2 Activate Rule
A Global MAC Rule will not be applied to the selected slot(s)/port(s) unless it is activated. Use the pull-down menu to select either yes or no. Default is no.

5.2.2.3 MAC Range
Packets containing a source and/or destination MAC address that falls within the configured range will match the MAC portion of the MAC Rule. Default is 00:00:00:00:00:00 - 00:00:00:00:00:00. No packets will match at the default MAC Range setting; you must configure the MAC Range as is appropriate for your individual network.

5.2.2.3.1 Single MAC Address
Only packets with the specified MAC address, as either their source or destination, will match the MAC address portion of the MAC Rule.

5.2.2.3.2 MAC Range
Only packets with a source and/or destination MAC address within the specified range will match the MAC address portion of the MAC Rule.

5.2.2.4 Allow Tag or Untag on Ingress Packets
Use the pull-down menu to select either tag or untag. Tag indicates that ingress packets already matched to the MAC Rule must have a VLAN tag to be further considered; packets without a VLAN tag will be dropped. Untag indicates that ingress packets already matched to the MAC Rule cannot have a VLAN tag to be further considered; packets with a VLAN tag will be dropped. Default is untag.
5.2.2.5 VLAN
For each individual MAC Rule, if you selected tag in Section 5.2.2.4, the VLAN field should specify either an acceptable Single VLAN, or an acceptable VLAN Range, for VLAN tags on ingress packets. If you selected untag, the VLAN field should specify a Single VLAN only if you intend to have a VLAN tag added to packets (Section 5.2.2.6); if you do not intend to have a VLAN tag added to packets, the VLAN field should be left at the 0 - 0 default.

5.2.2.5.1 Single VLAN
If tag was selected in Section 5.2.2.4, only packets with the specified VLAN tag will match the VLAN portion of the MAC Rule. If untag was selected, a Single VLAN should only be specified if the MAC Rule is also configured to add a VLAN tag to packets (Section 5.2.2.6).

For a packet that has already been matched to a MAC Rule:

<table>
<thead>
<tr>
<th>Start Tag = End Tag</th>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td>999 999</td>
<td>tag</td>
<td>no VLAN tag</td>
<td>match</td>
<td>have the configured VLAN tag added</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>untag</td>
<td>no VLAN tag</td>
<td>match</td>
<td>keep the same VLAN tag</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any VLAN tag other than the specified VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
</tr>
</tbody>
</table>

5.2.2.5.2 VLAN Range
A VLAN range should only be specified if tag was selected in Section 5.2.2.4. Only packets tagged within the specified VLAN range will match the VLAN portion of the MAC Rule. If a VLAN Range is specified, the MAC Rule MUST be configured to allow packets to continue on with the same VLAN tag they came in with (Section 5.2.2.6).
5.2.2.6  Add VLAN Tag to Ingress Packets

Use the pull-down menu to select either yes or no. Default is no.

For a packet that has already been matched to a MAC Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td>no VLAN tag</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>any VLAN tag within the specified range</td>
<td>match</td>
<td>keep the same VLAN tag</td>
<td></td>
</tr>
<tr>
<td>any VLAN tag not in the specified range</td>
<td>no match / packet dropped</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

For a packet that has already been matched to a MAC Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the MAC Rule must be configured with a single VLAN (Section 4.2.2.4.1) and a VLAN tag with the specified value will be added to the packet</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>the packet will continue on without a VLAN tag</td>
</tr>
<tr>
<td>tag</td>
<td>yes*</td>
<td>the packet will continue on with the same VLAN tag it had at ingress</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 5.2.2.4).

5.2.2.7  Priority

Use the pull-down menu to select a priority value from 0 - 7, where 0 is no priority, 1 is the lowest priority and 7 is the highest priority. Default is 0.
For a packet that has come in through a subscriber connection and has already been matched to a MAC Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the MAC Rule Priority will be added to the packet as part of the VLAN tag and will be applied to the packet both within the DSLAM and at egress</td>
</tr>
<tr>
<td>no</td>
<td></td>
<td>the packet will follow the MAC Rule Priority within the DSLAM only; it will not be added to the packet at egress</td>
</tr>
<tr>
<td>tag</td>
<td>yes*</td>
<td>Priority will be applied according to the MAC Rule Fixed/Max configuration (Section 5.2.2.8)</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 5.2.2.4).

**NOTE** MAC Rule Priority configurations do not apply to packets that have come in through an uplink connection; packets coming from an uplink connection will retain their original priority.

5.2.2.8 Fixed or Maximum Priority

The Fixed/Max field dictates the action to be taken with the configured Priority (Section 5.2.2.7) of a tagged packet that has come in through a subscriber connection and has already been matched to a MAC Rule. Use the pull-down menu to select either fixed or max. Default is fixed.

5.2.2.8.1 Fixed (default)

The packet’s original priority will automatically be replaced with the MAC Rule Priority (Section 5.2.2.7).

5.2.2.8.2 Max

The packet’s original priority will only be replaced with the configured MAC Rule Priority (Section 5.2.2.7) if the packet’s original priority is greater than the MAC Rule Priority. E.g. If the MAC Rule Priority has been configured at 4, a packet’s original priority will be replaced only if it is greater than 4 (as in 5, 6 or 7).

**NOTE** The MAC Rule Fixed/Max parameter does not apply to packets that have come in through an uplink connection; neither will the Fixed/Max configuration come into play if a QoS Backbone VLAN ID (Section 5.3.3.2) has been configured.

5.2.2.9 Ingress and Egress Limits

Ingress Limit and Egress Limit allow traffic-specific, rule-specific, bandwidth limits to be set for each port. Unit of measure is kbps. Default is 0 (no limit).
5.2.2.10  Matching Packets with a MAC Rule

The first step in matching a packet with a MAC Rule is matching the destination and/or source MAC address. Once it has been determined that a packet’s destination and/or source MAC address matches the configured single MAC or MAC range of a MAC Rule, it must then match all other criteria for that rule as well, or the packet will be dropped. If a packet’s destination and/or source MAC address does not match the single MAC or MAC range of a MAC Rule, the packet will be passed on for an attempted match with the next rule in line.

**NOTE**  If a packet’s destination and/or source MAC address matches the single MAC or MAC range of a MAC Rule but fails to match one or more of the other criteria for that rule, it will be dropped; it will not continue on to the next rule.

5.2.2.10.1  Packets with a VLAN Tag

When Allow Tag/Untag on Ingress Pkt. is set to *tag* (Section 5.2.2.4), a tagged packet with a MAC address and VLAN that match the configurations of a MAC Rule will be deemed a match with that rule and no further attempts will be made to match that packet with any other QoS Rules. Additionally, once a packet has been matched with a MAC Rule, it will conform to the priority and bandwidth limits as configured for that rule.

5.2.2.10.2  Packets without a VLAN Tag

When Allow Tag/Untag on Ingress Pkt. is set to *untag* (Section 5.2.2.4), an untagged packet with a MAC address that matches the configurations of a MAC Rule will be deemed a match with that rule and no further attempts will be made to match that packet with any other QoS Rules. Additionally, once a packet has been matched with a MAC Rule, it will conform to the VLAN and priority configurations, as well as bandwidth limits, as configured for that rule.

*If a QoS Rule Backbone VLAN has been configured, then the Backbone VLAN will be taken into consideration along with the standard VLAN in determining whether a packet matches a MAC Rule. Refer to Section 5.3.3.2 for further information regarding Backbone VLAN.*
5.2.3 Submit Global MAC Rules

Once all parameters in the Circuit Configuration MAC Rules window have been configured as desired, click the submit button at the bottom of the window. Any configurations that are not submitted will be discarded. If any accidental or undesirable changes have been made, exit the screen without clicking submit and the changes will be discarded. If any accidental or undesirable changes have already been submitted, simply make the desired adjustments and then resubmit the rule.

5.2.4 Reset Global MAC Rules

Resetting a port's MAC Rules will return ALL of that port's MAC Rules to their original default settings. Click the box to the left of the Reset until a check mark appears, then click submit.
5.3 Global VLAN Rules

Click on the Global VLAN Rules tab at the top of the Global Set window.

5.3.1 Select Slot(s) and Port(s) for Configuration

5.3.1.1 Slot

Using the pull-down menu, select the slot number of the interface module for which you wish to configure a VLAN Rule. The Slot pull-down menu will only list
the DSLAM slots that are occupied by an interface module; empty slots and slots occupied by blank plates will not be listed. The slot selected will be detailed in the Device Type and Revision fields. In the following illustration, there are interface modules in slots 1 and 2; Slot 2 has been selected and contains a SIM2000-24 with firmware revision 2.00.00.

<table>
<thead>
<tr>
<th>Slot</th>
<th>Device Type</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>SIM2000-24</td>
<td>2.00.00</td>
</tr>
</tbody>
</table>

**NOTE** There is no Slot selection field in the NMS Global Set window for Net to Net's Micro and Mini DSLAMs, only a Port selection field.

### 5.3.1.2 Add Slot(s)

After clicking the initial slot number in the Slot pull-down menu, hold down the "Ctrl" key on your keyboard to click (select) additional slot numbers (IP DSLAMs only). The additional slot numbers will appear in the field under Add Slot(s).

**NOTE** When configuring multiple interface modules at one time, all chosen modules must be of the same model type; NMS will not allow selection of different interface module models. Firmware versions may vary amongst the chosen slots however, as long as the models are the same.

<table>
<thead>
<tr>
<th>Slot</th>
<th>Add Slot(s)*</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

As illustrated here (and in Section 5.3.1.1), Slot 2 was the first slot selected; Slot 1 has been "added". Since the interface module in Slot 2 is a SIM2000-24 (as illustrated in Section 5.3.1.1) the interface module in Slot 1 must also be a SIM2000-24.

### 5.3.1.3 Add Port(s)

Ports may be selected singly, in multiples, or all at once. To select a single port, click on the number of the port you wish to configure. Hold down the "Ctrl" key on your keyboard to click (select) additional port numbers. Scroll down the Add Port(s) menu, if necessary, to access all of the port numbers you wish to select. To select ALL ports, click All. The port selections you make will apply to all of the previously selected interface modules (Section 5.3.1.1 and 5.3.1.2).

<table>
<thead>
<tr>
<th>Add Port(s)*</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
</tr>
</tbody>
</table>

In this illustration ALL ports have been selected. As applied to the example in Section 5.3.1.2, a configured Global VLAN Rule will be applied to all ports in both Slot 1 and Slot 2.

### 5.3.2 Global Configuration VLAN Rules

Virtual Local Area Network (VLAN) tag ranges are a method of providing OSI Layer 2 identification information for prioritization purposes. Packet priority is assigned based on the packet's VLAN tag. Up to ten [10] separate VLAN Rules may be configured per port.
Default on all ports is for one VLAN Rule to be activated with all parameters at default settings (as shown below): no DiffServ, IP Range or MAC Rules are activated by default. An activated VLAN Rule that has been left at default settings will allow all untagged packets to be forwarded (with no priority) and, if no additional QoS Rules are activated, all tagged packets will be dropped.

<table>
<thead>
<tr>
<th>VLAN Rules</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Activate Rule</td>
</tr>
<tr>
<td>1</td>
<td>yes</td>
</tr>
</tbody>
</table>

5.3.2.1 Add, Delete or Do Not Set

Global VLAN Rules can be added or deleted, they cannot be modified. If you wish to change a rule that has already been added, you will need to delete that rule and then add a new rule with the desired change(s).

5.3.2.1.1 Add

Add indicates that you wish to add a VLAN Rule to the selected slot(s)/port(s).

5.3.2.1.2 Delete

Delete indicates that you wish to remove a VLAN Rule that was previously applied to the selected slot(s)/port(s). In order to successfully delete a Global VLAN Rule, the configurations for EVERY FIELD must exactly match that of the rule you wish to delete.
5.3.2.1.3 *Do Not Set* (default)

*No Set* simply maintains the status quo of a Global VLAN Rule: as the default setting, it ensures that a Global VLAN Rule will not be added to, or deleted from, any slot(s)/port(s) without deliberate specification.

5.3.2.2 *Activate Rule*

A Global VLAN Rule will not be applied to the selected slot(s)/port(s) unless it is activated. Use the pull-down menu to select either *yes* or *no*. Default is *no*.

5.3.2.3 *Allow Tag or Untag on Ingress Packets*

Use the pull-down menu to select either *tag* or *untag*. *Tag* indicates that only ingress packets with a VLAN tag will be considered; all ingress packets without a VLAN tag will be passed on for an attempted match with the next VLAN Rule in line. *Untag* indicates that only ingress packets without a VLAN tag will be considered; all ingress packets with a VLAN tag will be passed on for an attempted match with the next VLAN Rule in line. Default is *untag*.

5.3.2.4 *VLAN*

For each individual VLAN Rule, if you selected *tag* in Section 5.3.2.3, the VLAN field should specify either an acceptable Single VLAN, or an acceptable VLAN Range, for VLAN tags on ingress packets. If you selected *untag*, the VLAN field should specify a Single VLAN only if you intend to have a VLAN tag added to packets (Section 5.3.2.5); if you do not intend to have a VLAN tag added to packets, the VLAN field should be left at the *0 - 0* default.

**NOTE**  
If you are unsure of one or more of the settings for a rule you wish to delete, you may view all of that rule’s configured parameters by returning to the main window, clicking on the depicted LED for one of the ports to which the rule is currently applied, and then clicking on the VLAN Rules tab at the top of the Circuit Configuration window; all VLAN Rules associated with that port will be listed along with their individual parameter settings.

**NOTE**  
No more than one VLAN Rule per port should be configured to allow packets without a VLAN tag (*untag*); any untagged packets that have not already been matched to a DiffServ, IP Range or MAC Rule will automatically be matched with the FIRST VLAN Rule that allows untagged packets. Therefore, any subsequent VLAN Rules allowing untagged packets will not be utilized.
5.3.2.4.1 Single VLAN
If *tag* was selected in Section 5.3.2.3, only packets with the specified VLAN tag will match the VLAN Rule. If *untag* was selected, a Single VLAN should only be specified if the VLAN Rule is configured to add a VLAN tag to packets (Section 5.3.2.5).

### Table: VLAN Tag/Untag on Ingress Pkt.

<table>
<thead>
<tr>
<th>VLAN (1-4085)</th>
<th>Start Tag = End Tag</th>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td>999</td>
<td><strong>untag</strong></td>
<td>no VLAN tag</td>
<td>match</td>
<td>have the configured VLAN tag added</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>any VLAN tag</td>
<td>no match; packet will be passed on for an attempted match with the next VLAN Rule in line</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>no VLAN tag</td>
<td>no match; packet will be passed on for an attempted match with the next VLAN Rule in line</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the specified VLAN tag</td>
<td>match</td>
<td>keep the same VLAN tag</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>any VLAN tag other than the specified VLAN tag</td>
<td>no match; packet will be passed on for an attempted match with the next VLAN Rule in line</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

5.3.2.4.2 VLAN Range
A VLAN range should only be specified if *tag* was selected in Section 5.3.2.3. Only packets tagged within the specified VLAN range will match the VLAN Rule. If a VLAN Range is specified, the VLAN Rule MUST be configured to allow packets to continue on with the same VLAN tag they came in with (Section 5.3.2.5).

### Table: VLAN Tag/Untag on Ingress Pkt.

<table>
<thead>
<tr>
<th>VLAN (1-4085)</th>
<th>Start Tag &lt; End Tag</th>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and the ingress packet has</th>
<th>the result will be</th>
<th>and the egress packet will</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>tag</strong></td>
<td>no VLAN tag</td>
<td>no match; packet will be passed on for an attempted match with the next VLAN Rule in line</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td></td>
<td>any VLAN tag within the specified range</td>
<td>match</td>
<td>keep the same VLAN tag</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>any VLAN tag not in the specified range</td>
<td>no match; packet will be passed on for an attempted match with the next VLAN Rule in line</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>
5.3.2.5  Add VLAN Tag to Ingress Packets

Use the pull-down menu to select either yes or no. Default is no.

For a packet that has already been matched to a VLAN Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the VLAN Rule must be configured with a single VLAN (Section 5.3.2.1) and a VLAN tag with the specified value will be added to the packet.</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>the packet will continue on without a VLAN tag.</td>
</tr>
<tr>
<td>tag</td>
<td>yes*</td>
<td>the packet will continue on with the same VLAN tag it had at ingress.</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 5.3.2.3).

5.3.2.6  Priority

Use the pull-down menu to select a priority value from 0 - 7, where 0 is no priority, 1 is the lowest priority and 7 is the highest priority. Default is 0.

For a packet that has come in through a subscriber connection and has already been matched to a VLAN Rule:

<table>
<thead>
<tr>
<th>if Allow Tag/Untag on Ingress Pkt. is configured as</th>
<th>and Add VLAN to Ingress Pkt. is configured as</th>
<th>then</th>
</tr>
</thead>
<tbody>
<tr>
<td>untag</td>
<td>yes</td>
<td>the VLAN Rule Priority will be added to the packet as part of the VLAN tag and will be applied to the packet both within the DSLAM and at egress.</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>the packet will follow the VLAN Rule Priority within the DSLAM only; it will not be added to the packet at egress.</td>
</tr>
<tr>
<td>tag</td>
<td>yes*</td>
<td>Priority will be applied according to the VLAN Rule Fixed/Max configuration (Section 5.3.2.7).</td>
</tr>
</tbody>
</table>

*Add VLAN to Ingress Pkt. must be configured as yes when tagged packets are allowed (Section 5.3.2.3).
5.3.2.7 Fixed or Maximum Priority
The Fixed/Max field dictates the action to be taken with the configured Priority (Section 5.3.2.6) of a tagged packet that has come in through a subscriber connection and has already been matched to a VLAN Rule. Use the pull-down menu to select either fixed or max. Default is fixed.

5.3.2.7.1 Fixed (default)
The packet's original priority will automatically be replaced with the VLAN Rule Priority (Section 5.3.2.6).

5.3.2.7.2 Max
The packet's original priority will only be replaced with the configured VLAN Rule Priority (Section 5.3.2.6) if the packet's original priority is greater than the VLAN Rule Priority. E.g. If the VLAN Rule Priority has been configured at 4, a packet's original priority will be replaced only if it is greater than 4 (as in 5, 6 or 7).

5.3.2.8 Ingress and Egress Limits
Ingress Limit and Egress Limit allow traffic-specific, rule-specific, bandwidth limits to be set for each port. Unit of measure is kbps. Default is 0 (no limit).

5.3.2.9 Matching Packets with a VLAN Rule
The first step in matching a packet with a VLAN Rule requires a determination of whether or not the packet has a VLAN tag. If the VLAN Rule has been configured to allow only tagged packets, then all untagged packets will be passed on for an attempted match with the next VLAN Rule in line, as will any tagged packets with a VLAN tag falling outside of the configured range (Section 5.3.2.4). If the VLAN Rule has been configured to allow only untagged packets, then all tagged packets will be passed on for an attempted match with the next VLAN Rule in line.

5.3.2.9.1 Packets with a VLAN Tag
When Allow Tag/Untag on Ingress Pkt. is set to tag (Section 5.3.2.3), then any packet having a VLAN tag within the configured range (Section 5.3.2.4) will be deemed a match with that VLAN Rule and no further attempts will be made to match that packet with any other VLAN Rules. Additionally, once a packet has been matched to a VLAN Rule, it will conform to the priority and bandwidth limits as configured for that rule.
5.3.2.9.2 Packets without a VLAN Tag
When Allow Tag/Untag on Ingress Pkt. is set to untag (Section 5.3.2.3) then all packets without a VLAN tag will be deemed a match with that VLAN Rule and no further attempts will be made to match those packets with any other VLAN Rules. Additionally, once a packet has been matched with a VLAN Rule, it will conform to the priority configurations and bandwidth limits of that rule.

If a QoS Rule Backbone VLAN has been configured, then the Backbone VLAN will be taken into consideration along with the standard VLAN in determining whether a packet matches a VLAN Rule. Refer to Section 5.3.3.2 for further information regarding Backbone VLAN.

No more than one VLAN Rule per port should be configured to allow packets without a VLAN tag; any untagged packets that have not already been matched to a Diffserv, IP Range or MAC Rule will automatically be matched with the FIRST VLAN Rule that allows untagged packets. Therefore, any subsequent VLAN Rules allowing untagged packets will not be utilized.

5.3 Backbone and Flood
Backbone Ethertype, Backbone VLAN Identification (ID) and Flood, as configured here, apply to ALL QoS Rules: Diffserv Rules, IP Range Rules, MAC Rules and VLAN Rules. These parameters cannot be applied on their own; there must be at least one QoS rule activated. To this end, one VLAN Rule is activated as a QoS default; refer to Section 5.3.2 for a description.
5.3.3.1 Backbone Ethertype
Backbone Ethertype is a two-byte code indicating packet type. Use the pull-down menu to select either 8100 or 9100; selection should be based on the type of packets supported by your router. Default is 8100.

5.3.3.2 Backbone VLAN ID
Used in conjunction with standard VLAN tags, a single Backbone VLAN tag will become the primary identifier, allowing a router with backbone capabilities to make smarter decisions in directing traffic to the proper network. Once a packet has reached the proper network, its standard VLAN tags will direct it to the appropriate port. To configure Backbone VLAN ID, enter a single VLAN tag value between 0 and 4085. Default is 0, indicating that the Backbone VLAN function is not in use.
For a packet that has already been matched with a QoS Rule:

<table>
<thead>
<tr>
<th>ingress packets from the</th>
<th>with</th>
<th>will be _____ when Backbone VLAN IS configured</th>
<th>will be _____ when Backbone VLAN IS NOT configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>subscriber (WAN)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>both Backbone VLAN and standard VLAN tags only</td>
<td>DROPPED regardless of whether the packet's Backbone VLAN tag is in accordance with current configurations.</td>
<td>DROPPED</td>
<td></td>
</tr>
<tr>
<td>standard VLAN tags only</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched. A Backbone VLAN tag with the QoS Rule Priority will be added prior to transmission (the standard VLAN tag will maintain the Priority configuration the packet had at ingress).</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched.</td>
<td></td>
</tr>
<tr>
<td>no VLAN tags: neither Backbone VLAN nor standard VLAN</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched. A Backbone VLAN tag and a standard VLAN tag, both with the QoS Rule Priority, will be added to the packet prior to transmission.</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched. A standard VLAN tag with the QoS Rule Priority will be added prior to transmission.</td>
<td></td>
</tr>
<tr>
<td>uplink</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>both Backbone VLAN and standard VLAN tags only</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched as long as the packet's Backbone VLAN tag matches the QoS Rule's Backbone VLAN configuration. The Backbone VLAN tag will be stripped prior to packet transmission. The packet will be DROPPED if its Backbone VLAN tag does not match the QoS Rule's Backbone VLAN configuration.</td>
<td>DROPPED</td>
<td></td>
</tr>
<tr>
<td>standard VLAN tags only</td>
<td>DROPPED</td>
<td>TRANSMITTED in accordance with the VLAN portion of the QoS Rule to which the packet has been matched. A standard VLAN tag with the QoS Rule Priority will be added prior to transmission.</td>
<td></td>
</tr>
</tbody>
</table>

*The Fixed/Max configuration of a QoS Rule will not come into play when a Backbone VLAN ID has been configured.

**NOTE**
A Backbone VLAN tag cannot be used independently; standard VLAN tags must also be configured. Additionally, the DSLAM uplink connection must run through a router in order for a Backbone VLAN tag to function.

5.3.3.3 Flood
Flood refers to the method in which interface modules handle unknown unicasts (traffic directed to a single MAC address), broadcasts (traffic directed to all MAC addresses) and multicasts (traffic directed to multiple MAC addresses) for each port. Use the pull-down menu to select either Upl (uplink) or Vln (VLAN: access ports). Default is Upl.

5.3.3.3.1 Uplink (default)
Unknown unicast, broadcast and multicast traffic will be flooded to the DSLAM uplink interface ports, preventing communication between interface ports without the intervention of an upstream device such as a router. If
communication between interface ports is desired, the upstream device must be properly configured to allow it.

5.3.3.2 VLAN
Unknown unicast, broadcast and multicast traffic will be flooded to both DSLAM access ports (within the sender’s VLAN range) and the uplink interface ports.

5.3.4 Submit Global VLAN Rules
Once all parameters in the Global Set VLAN Rules window have been configured as desired, click the submit button at the bottom of the window. Any configurations that are not submitted will be discarded. If any accidental or undesirable changes have been made, exit the screen without clicking submit and the changes will be discarded. If any accidental or undesirable changes have already been submitted, you must delete the affected rule and then create a new rule with the desired settings; refer to Section 5.3.2.1.

5.3.5 Reset Global VLAN Rules
Resetting a port’s VLAN Rules will return ALL of that port’s VLAN Rules to their original default settings. Click the box to the left of the Reset until a check mark appears, then click submit.
Reset the VLAN rules to default parameters for the slot(s) and port(s) selected.

**NOTE** A reset will not take place unless it is submitted.